MITEL

COMMUNICATIONS DIRECTOR

TROUBLESHOOTING GUIDE
MITEL COMMUNICATIONS DIRECTOR RELEASE 6.0 SP1

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

Troubleshooting Guide
Mitel Communications Director (MCD) Release 6.0 SP1
Rev. A

May 2013

Chapter 1: Introduction

About this Guide 3

Supporting Documentation 3

Accessing Mitel OnLine 3

Access eDocs for the Latest Documentation 3

Resolving Technical Issues 5

TSN: Your Technical Support Network 8

Registering for Services 9

What Services are Available? 9

What Products are Supported? 11

Summary of Service Charges 12

Self Help Solutions 12

Checking the Knowledge Base 12

Using the Online Service Desk (OSD) 13

Checking for Fixes in Software Patches 13

Fixed in Latest Software Patch? 13

Fixed in Previous Software Patch? 14

Fixed in Software Update? 14

Accessing Product Support 15

Before You Call 15

Making a Support Call 19

What are Normal Business Hours? 19

What are After-Hours Calls? 19

Emergency Calls are Not Charged 20

Returning Faulty Hardware 21

Chapter 2: Initial Setup

Initial Setup Troubleshooting Tips 25

All Controllers 25

AX, MXe, CX, or CXi Controller 25

MXe Server Setup 28

Licensing 29

Chapter 3: Hardware

Hardware Troubleshooting Tips 35
Hardware Alarms 36
Controllers 39
MXe Controller 39
CX/CXi Controller 40
MXe Server 41
Service Units 44
Gateways 47
Peripheral Cabinets 47
Embedded Modules 50
Phones 53
General Phone Issues 53
Issues with Specific Models 59
IP Phone Power 65
IP Phone Registration 69
Phone Connection 77
Phone Audio Quality 78
5550 IP Console 82

Chapter 4: Software

Software Troubleshooting Tips 87
System Software 87
Software Installation and Upgrade 88
Backups and Restores 90

Chapter 5: System Features

System Feature Troubleshooting Tips 97
Features A to B 98
Features C 100
Features D to G 104

Features H to K. 107
Features L to O. 108
Features P to R. 110
Features S to V. 111

Chapter 6: Trunking

Trunk Troubleshooting Tips 115
Analog Trunks. 115
Digital Trunks 118
MSDN/DPNSS Links 125
XNET 127
IP Trunking (IP Networking) 129
SIP Trunking. 130

Chapter 7: Tools and Embedded Applications

System Management Tools 132
Automatic Call Distribution 140
Hot Desking 141
Emergency Call (E911) Support. 141
Embedded Voice Mail. 142
Networked Voice Mail. 149
Station Message Detail Recording 151
Unified IP Client for Sun Ray 152

Chapter 8: Voice Networking

Voice Networking Troubleshooting Tips. 155
Bandwidth Management. 155
Clustering 155
IP Networking 155

Multi-Node Management. 156
MNM Fault Management 156
MNM Backup and Restore 157
MNM Application Reach Through 157

Resiliency 159
IP Device Resiliency 159
IP Console Resiliency 165
Voice Mail Resiliency 166
T1/E1 Trunk Resiliency 167

System Data Synchronization. 168
Sharing Operations 168
Sync Operations 173
Hunt Group or Ring Group Data Distribution Errors 175

Chapter 9: Local Area Network

LAN Troubleshooting Tips 179

LAN Troubleshooting 180

Using Layer 2 Statistics 181
Shared versus Switched LANs 181
Collisions 182
Shared LANs 182
Switched LANs 182
CRC/FCS & Alignment Errors 182
Frame Length Errors 182

Chapter 10: Diagnosing Problems

Diagnostic Tools 189

Phones 191
Diagnosing Phone Problems 191
No Dial Tone - Analog or DNI Phone 191
No Dial Tone - IP Phone 193
Viewing Settings and Network Parameters on IP Phones 193
Access Configuration Menu on Single-Mode IP Phones 194
Access Configuration Menu on Dual Mode Phones and 5235 IP Phones 194
Viewing/Modifying Network Parameters 195
Configuring Hardware Components 196

Setting the Phone Mode 197
Using Tools and Features 197
IEEE 802.1X Authentication for IP Phones 199
Configuring an Authentication Username and Password 199
Erasing an Authentication Username and Password 200
Enabling or Disabling 802.1X Authentication 201
IP Phone Boot Sequence 201
Checking the IP Phone Resiliency Progress Display 206
Diagnosing SIP Device Issues 207

Trunks 209
Diagnosing Digital Trunk Issues 209

Hardware 211
Using LEDs to Diagnose Faults 211
R2 Card Debugging 211
Reading E2T Card Statistics 212
Diagnosing DSP Module Related Issues 214
Diagnosing Formatter Card Problems 214
Diagnosing MSDN/DPNSS Link Problems 214
Loopback Testing on Digital Trunks 215

Resiliency 217
Locating Resilient Devices 217
Locate Extension 217
Locate Feature 219
Locate Remote 219
Locating Resilient Hunt Groups 220
Identifying the Status of a Resilient Device 221
State Extension 221
State XNET ICP 222
Obtaining the Status of Resilient Trunks 222
Controlling the Failover and Failback of Resilient Trunks 222
Identifying the Current ICP 223
Checking T1/E1 Resiliency Alarms 223
Checking the T1/E1 Combo MMC Indicators 224

Chapter 11: Using Logs

Logs 229
Software Logs for System Features 229
Hot Desking Error Logs 230
Voice Mail System Logs 231
Index 247

CHAPTER 1

INTRODUCTION

About this Guide

This guide provides troubleshooting information for the Mitel® 3300 IP Communications Platform (ICP). This guide is intended for use by Mitel certified 3300 ICP technicians.

The troubleshooting information has been grouped by topic (Initial Setup, System Features, Devices, and so forth) and then organized into tables using the following structure:

- Symptom,
- Probable Cause, and
- Corrective Action.

To locate help on a on a specific problem

- use the Adobe Acrobat search functionality to search on key words associated with the problem symptoms, or
- go to the table that contains troubleshooting information related to the problem and scan the symptoms column for a possible match.

Supporting Documentation

This guide references other documents that are available on Mitel Online and on the Mitel Customer Documentation web site.

Accessing Mitel OnLine

To access Mitel OnLine

1. Go to the following URL: **http://www.mitel.com**
2. Click **Login.**
3. Enter your Mitel Online username and password.

Note: To fully utilize Mitel OnLine including the available training and documentation, you will require high-speed internet access and a web browser. As well, you should have Adobe Acrobat Reader 4.0 or later and Microsoft Word 97 or later.

4. Click **Login**.

Access eDocs for the Latest Documentation

The Mitel Customer Documentation (eDocs) site on Mitel OnLine provides the latest customer documentation.

The documentation for the current and previous product release are available from the main page. The documentation for other past releases are available from the Documentation Library link.

To view the available documentation, you will require

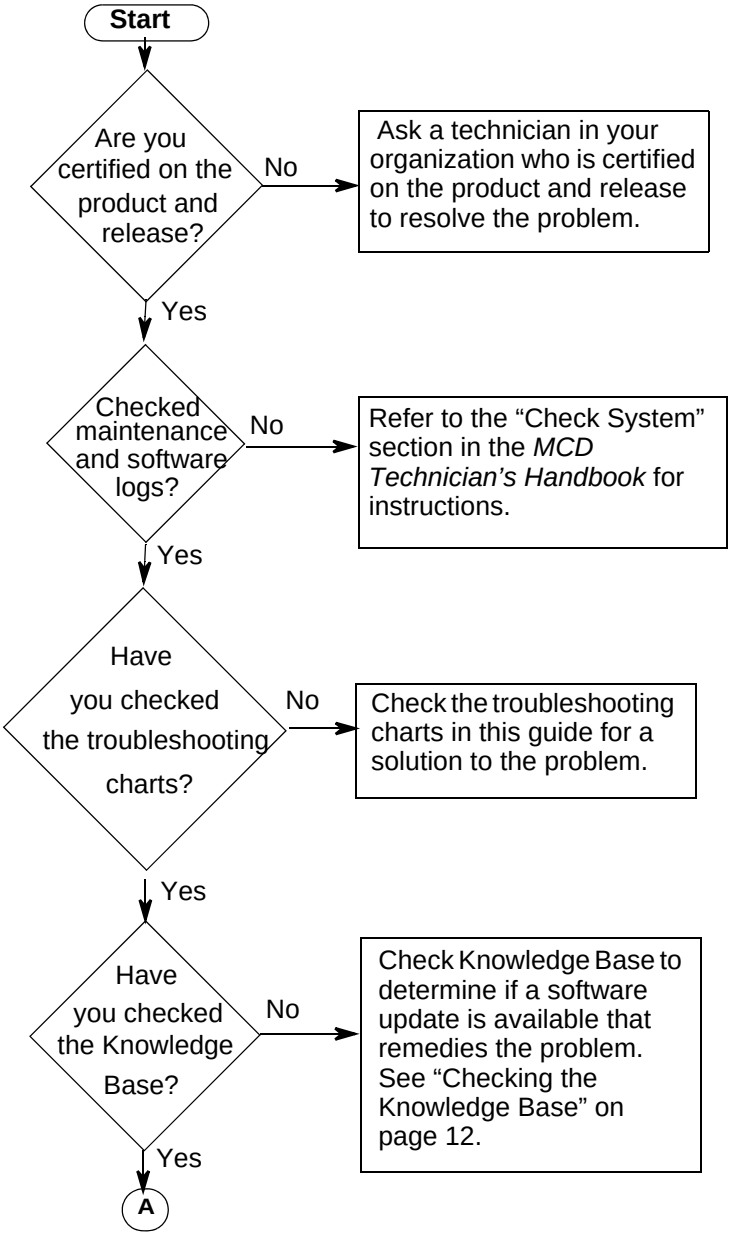
- Internet access (high-speed is recommended)
- a web browser (e.g., Internet Explorer 7.0 or later)
- Adobe Acrobat Reader 4.0 or later
- Microsoft Word 97 or later
- Folio (for SX-200 ICP, SX-200 EL/ML, or SX-2000 LIGHT)
- your Mitel OnLine user name and password (required to access technical documentation; user documentation is not password protected)

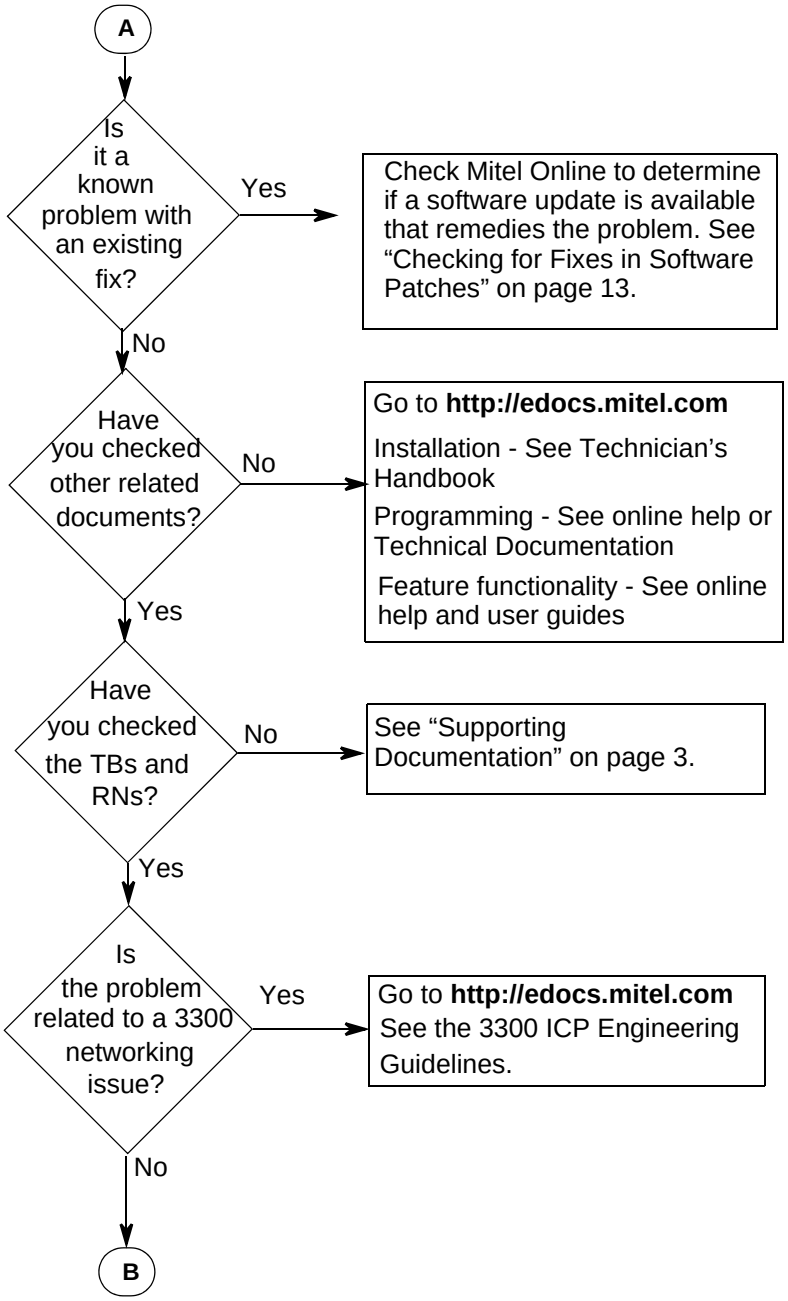
To access a technical document

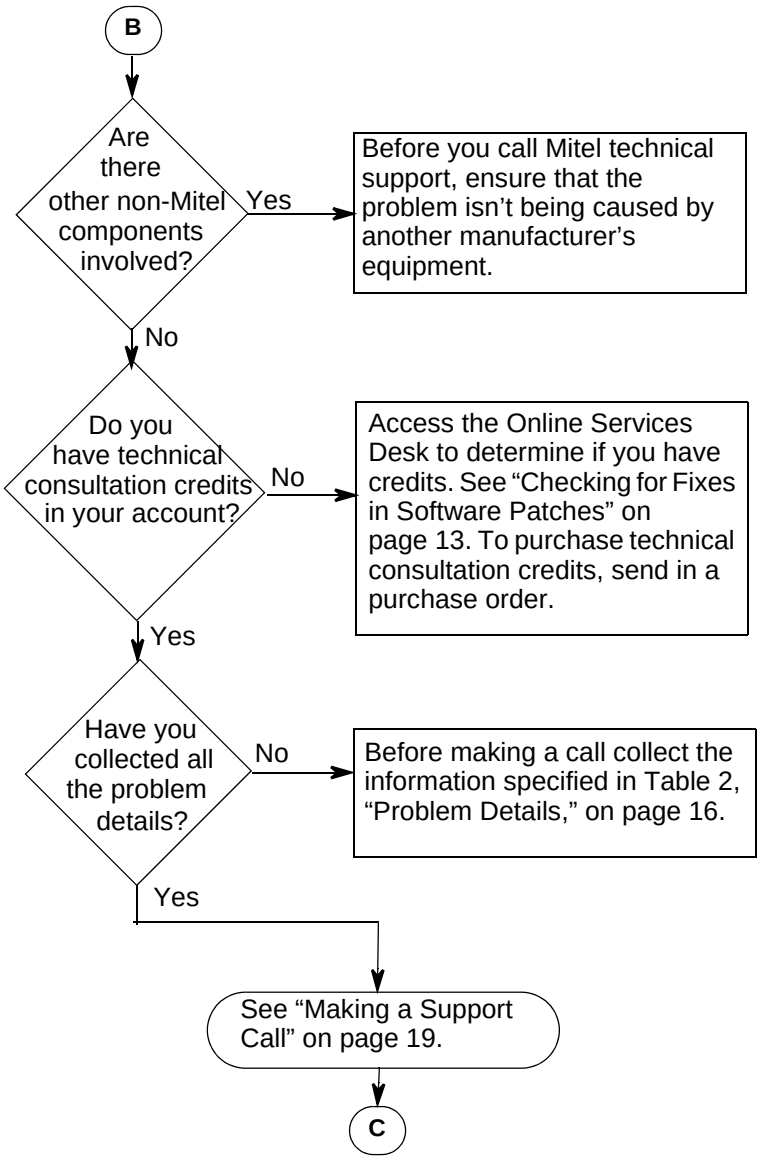
1. Log onto Mitel OnLine.
2. Click **Support** and then click **Product Documentation**.
3. Bookmark this URL.
4. In the left frame, select the product.
5. In the right frame, click the document.
6. If you click a technical document, you will be prompted for your Mitel OnLine username and password. Enter your username and password and click **Login**.
7. To access a generic user guide or quick reference card, click **User Guides**, click the desired language at the top of the frame, and then click the desired guide or quick reference card.

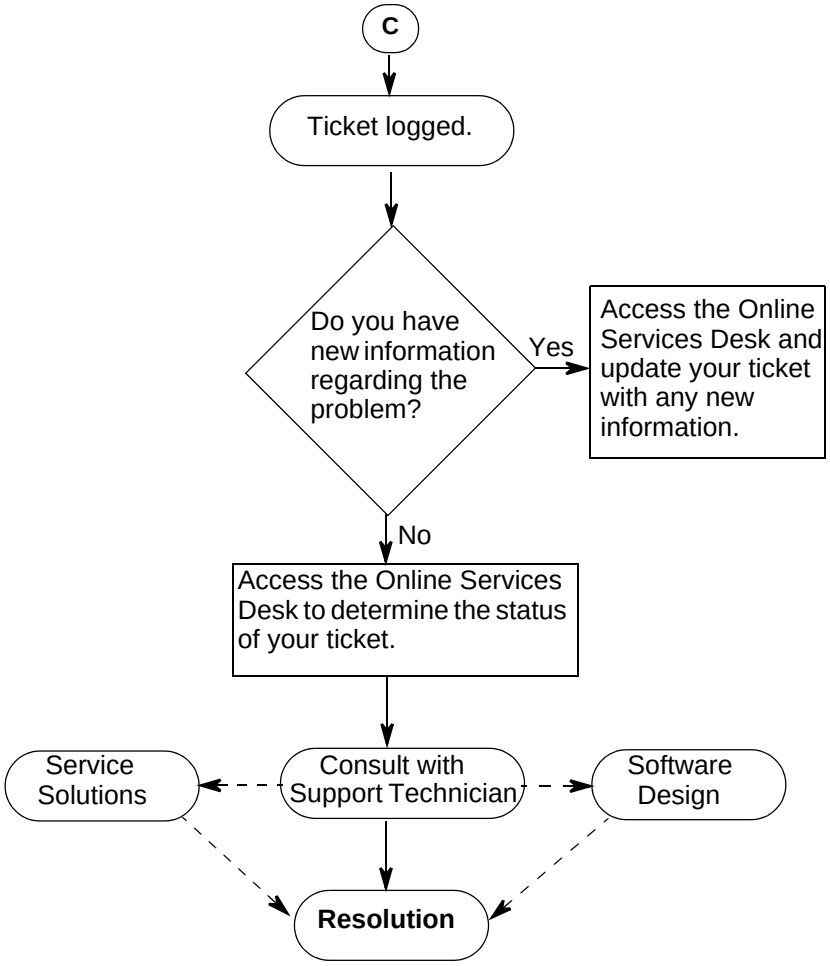
Resolving Technical Issues

Use the following flowchart to resolve technical issues:




A
Is it a known problem with an existing fix?
Yes
Check Mitel Online to determine if a software update is available that remedies the problem. See "Checking for Fixes in Software Patches" on page 13.
No
Have you checked other related documents?
No
Go to http://edocs.mitel.com
Installation - See Technician's Handbook
Programming - See online help or Technical Documentation
Feature functionality - See online help and user guides
Yes
Have you checked the TBs and RNs?
No
See "Supporting Documentation" on page 3.
Yes
Is the problem related to a 3300 networking issue?
Yes
Go to http://edocs.mitel.com
See the 3300 ICP Engineering Guidelines.
No
B


B
Are there other non-Mitel components involved?
Yes
Before you call Mitel technical support, ensure that the problem isn't being caused by another manufacturer's equipment.
No
Do you have technical consultation credits in your account?
No
Access the Online Services Desk to determine if you have credits. See "Checking for Fixes in Software Patches" on page 13. To purchase technical consultation credits, send in a purchase order.
Yes
Have you collected all the problem details?
No
Before making a call collect the information specified in Table 2, "Problem Details," on page 16.
Yes
See "Making a Support Call" on page 19.
C



TSN: Your Technical Support Network

The Mitel Technical Support Network (TSN) provides authorized channel partners with the following services:

- access through the Mitel OnLine website to
  - up-to-date customer documentation
  - the Mitel Knowledge Base
  - the Online Service Desk (OSD) allowing you to view and update your Technical Support Tickets
- standard telephone support with current product releases during normal business hours
- after-hours emergency telephone support
- e-mail notification of new and updated technical documentation.

Before you can become a registered user, you must purchase a minimum of five technical consultation credits. Your technical consultation credits can be used to purchase telephone support (standard and emergency).

Note: If you have questions about the Technical Support Network Program or your access to Technical Support, please call 1-613-592-2122 ext. 5140 or e-mail your question to tsn@mitel.com.

Note: To access TSN services, you must have a positive balance of technical consultation credits in your account.

Note: Online Service Desk (OSD) response time is three business days. The OSD should not be used to obtain emergency support services.

Registering for Services

To register for access to TSN services

1. Complete a Technical Consultation Order form and fax the form to Mitel Customer Services at 613-591-2308.
2. After the Mitel Customer Services receives your purchase order, we will fax a Technical Support Identification (TSID) code to the fax number that you included with your order form.
3. Distribute the TSID code to staff who require access to TSN services, including staff that may need to call Mitel Technical Support.

Note: Change your TSID code whenever you experience staff turnovers. You can change your TSID code at any time by contacting the Mitel TSN Coordinator:
Phone: 613-592-2122 extension 5140
E-mail: tsn@mitel.com

4. Instruct your staff to obtain a Mitel OnLine username and password by submitting a request online. All requests are confirmed with the designated channel partner. After a request is confirmed, a username and password is e-mailed to the individual.
5. Instruct your staff to register for the Online Service Desk. From Mitel OnLine, click **Technical Support**, then click **Online Service Desk** under Related Links. Complete and submit the form. Registrations will be processed within 2 business days (a return e-mail will confirm activation).

What Services are Available?

- **Mitel Knowledge Base:** provides access through the Mitel Online website to the latest product information. The Knowledge base provides
  - *Technical Bulletins (TBs)*: provide information on the installation and service of Mitel products. TBs are issued to introduce new software support tools, provide support information on discontinued products, identify product issues and describe TSN

program policies.TBs are published when required.

- *How to Articles*: provide information on proper programming of features and applications
- *Troubleshooting Articles*: provide troubleshooting procedures to help identify and solve issues.
- *Known Product Issues*: describe product issues that are know by Mitel and are in the process of being resolved.
- *Release Notes (RNs)*: provide software upgrade procedures, describe documentation and hardware requirements, summarize the new enhancements in a release, identify improvements that have been made in the product in response to customer reported issues, and include last-minute product changes that are not described in the latest documentation. RNs are published for each new software release.

- **E-mail Notification of new and updated TBs and RNs:** sends you an e-mail twice a month that identifies all the new and updated TBs and RNs. The e-mail includes URLs to each document. You can register for this optional service through Mitel OnLine. Log into Mitel OnLine, click **Technical**, and then click **Register/Cancel Email Notifications**.
- **Standard telephone support:** allows certified channel partner technicians to consult Mitel Network's Technical Support Specialists on current products during normal business hours. For details see "Making a Support Call" on page 19.

CAUTION: You will be charged for support calls if the technician making the call is not certified up to the software release of the system or if the call pertains to a product or software version that has been manufacture discontinued.

- **After-hours emergency telephone support:** outside of normal business hours, certified technicians can consult with a Technical Support Specialist or a Support Manager for assistance with resolving an emergency situation or with restoring service for an essential services site. See "What are After-Hours Calls?" on page 19 for details.
- **Online Service Desk (OSD):** allows you to view the status of your active Technical Support Tickets and your technical credit statement. Whenever changes are submitted against your account, you will be sent a confirmation email.To register for OSD notification updates, log into Mitel OnLine, click Technical, and then click **Register/Cancel Email Notifications**.
- **Password Resets:** if you lose your password or if your password is not available, Mitel can attempt to reset it for you. Password resets are chargeable and are subject to approval of our legal counsel. The end-customer must sign a Mitel approved form letter authorizing the reset. To obtain the required form letter, access Mitel Online, click **Support**, click **System Password Rests**. At the bottom of the web page, under **Resources**, click **Password Reset** and download the form letter. Complete a written request based on the form letter and e-mail it to TSN@Mitel.com.
- **Software Releases:** you can download the latest product software releases from Mitel Online. To access the available software downloads on Mitel Online, click Technical Support and then click Software Downloads.
- **Software Patches:** between major releases, you can download major system software patches from Mitel OnLine that include fixes for field-found problems (see "Checking for Fixes in Software Patches" on page 13). Note that minor software patches are only available from Technical Support via a Mitel FTP site.

- **Replacement of failed (out-of-box) system:** if a system fails within the first 72 hours of service it will be replaced by Mitel. Direct requests for replacement of failed systems to Mitel Customer Service Group. Replacements of defective software, complete systems, or three or more components of a system must be authorized by Mitel Technical Support.

What Products are Supported?

For an up-to-date list of the products that are supported, see the Technical Support Network Program Guide. You can access this guide through Mitel OnLine. From Mitel OnLine, click Technical Support, and then click Technical Support Network Program Guide under Downloads.

Telephone support falls into one of the following categories:

Current Products: Telephone support is provided at no charge during normal business hours to Mitel certified technicians for the currently supported products.

Manufactured Discontinued - Supported: Telephone support is chargeable for the manufacture discontinued products.

Manufactured Discontinued - Unsupported: Telephone support is not available for manufactured discontinued products. Access to all existing technical support bulletins for these products remains available through Mitel Online.

Summary of Service Charges

Table 1: Service Charges

Products	Free Support with subscription to Mitel TSN	Chargeable Support (Use TC credits to purchase)
Current (all software releases currently on Price List, excluding spares)	• Access to Mitel OnLine • Over the phone technical consultation for **product and release certified** technicians during normal business hours • Online Service Desk (OSD), view and update support tickets • After hours emergency consultation for certified technicians (see "Emergency Calls are Not Charged" on page 20 for details) • Technical consultation as a result of documented Mitel product defects (DPARs). • E-mail notification of all new updated technical support documents • Access to the Knowledge Base	• Over the phone technical consultation for **product certified** technicians during normal business hours (1 credit / hr / incident) • After hours support for non-critical situations (1.5 credit / hr / incident) • System access / system password reset, other special services (3 credits flat rate -- some conditions apply) **Note:** Telephone support will not be provided to technicians without certification in the subject product.
Discontinued (not on Price List)	• Access to the Knowledge Base	• Over the Phone tech consultation during normal business hours (1 credit / hr / incident) • After hours support for non-critical situations (1.5 credits / hr / incident)
Discontinued (not supported)	• Access to the Knowledge Base	There will be no telephone support for these products. In the event a system is totally out of service we will provide best effort support at a charge of 5 credits / hr.

Self Help Solutions

Checking the Knowledge Base

The Knowledge Base is your source for product information covering a large range of technical support methods. All new Technical Bulletins (TBs), Release Notes (RNs), How to Guides and Troubleshooting guides will be posted in the Knowledge Base. Access to the Knowledge Base is given with access to MOL.

To access the Knowledge Base:

1. Log into Mitel OnLine.
2. From Mitel OnLine, click **Technical** and then click **Knowledge Base**.

3. Select the product name (for example, 3300 Integrated Communications Platform).
4. Select the type of article you are looking for or choose **All**.
5. Click **Search**.

Using the Online Service Desk (OSD)

The Online Service Desk provides up-to-date information on your Support Notifications and Technical Credit balance. This portal lets you view the status of your open tickets, update Support Notifications with new information for our technical support team, and check your technical credit usage. Once the issue has been resolved your ticket will be updated. OSD will automatically display all active support notifications when you log in.

To access the Online Service Desk:

1. Log into Mitel OnLine.
2. From Mitel OnLine, click **Support**, then click **Online Service Desk**.
3. The first time you log in you will be asked for your company's Technical Support ID.
4. Choose your channel partner location.
5. View your open and closed tickets.
6. Update your open tickets with any new information and the Mitel technical support specialist will be notified of your updates by e-mail.

Note: Online Service Desk (OSD) response time is three business days. The OSD should not be used to obtain emergency support services.

7. Display a summary of your technical credits (depending on your access privileges).

Checking for Fixes in Software Patches

Before calling technical support with a problem, check to see if there is a software update available on Mitel Online that includes a fix for the problem.

- Major software patches are provided on Mitel Online.
- Minor software updates are available from Technical Support via a Mitel FTP site. The Known Product Issue (KPI) fixes that are contained in minor software updates are listed in the "KPI fixed lists" articles. The "KPI fixed lists" are Mitel Knowledge Base articles.

If an update is available with the required fix, you can download the software patch or update and install it on the system.

Fixed in Latest Software Patch?

To determine if a fix for your problem is available in the latest software patch:

1. Log into Mitel OnLine.
2. Click click **Technical** and then click **Software Downloads**.
3. Click the product name (for example, 3300 Integrated Communications Platform).
4. Click the latest software update.
5. Open the Release Notes (RN).
6. In the RN, review the list of problems that are resolved in this software update. If your required fix is listed, read the RN carefully to ensure that the update is appropriate, download the update, and then install it on the system. See the *MCD Technician's Handbook* for software installation instructions.

Fixed in Previous Software Patch?

If the software version on your system is a few releases old, the fix may have been provided in a previous software patch. To check the problems that have been fixed in previous software patches

1. Log into Mitel OnLine.
2. From Mitel OnLine, click **Technical**, and then click **Knowledge Base**.
3. Select the product name (for example, 3300 Integrated Communications Platform).
4. Set the Article Type to Release Notes (RN) and then click **Start Search**.
5. Open the RNs that have been issued since the release of your system's current software and check the list of problems that have been fixed.
6. If you find a fix to your problem, download and install the latest software patch. See the *MCD Technician's Handbook* for software installation instructions.

Fixed in Software Update?

To determine if a problem has been fixed in a minor software update:

1. Log into Mitel OnLine.
2. From Mitel OnLine, click **Technical**, and then click **Knowledge Base**.
3. Select the product name (for example, 3300 Integrated Communications Platform).
4. Enter "KPI" and then click **Start Search**.
5. Open and review the Known Product Issues (KPI) fixed lists.
6. If you find a fix to your problem, contact Technical Support to obtain the software update.

Accessing Product Support

Before You Call

1. Are you certified on the product in question?
2. Have you searched the tables in this Troubleshooting Guide for a solution?
3. Have you checked the Mitel Customer Documentation site, Knowledge Base and training materials for a solution to the issue?
4. Is the product supported (see “What Products are Supported?” on page 11)?
5. Do you have technical consultation credits available in your account (see “Summary of Service Charges” on page 12)? You can check your technical credit usage through the Online Service Desk (see “Using the Online Service Desk (OSD)” on page 13).
6. Do you have your valid TSID code at hand?
7. Are you calling within normal business hours or after hours? See “What are Normal Business Hours?” on page 19 and “What are After-Hours Calls?” on page 19.
8. Is it an emergency call? See “Emergency Calls are Not Charged” on page 20.
9. Have you collected the following information?

Table 2: Problem Details

Required Information	Details
Site information	Name, address, and phone number of end-user site
Product	What system or application is exhibiting the problem? What is the system or application variant (for example: 3300 ICP MXe or vMCD)?
Country variant	What country variant is selected for the controller?
Software version	What software version is the system running (for example, MCD Release 4.2 (10.2.2.10)?
System Identifier or Hardware Identifier	SysID code of system, and the ARID.
Serial number(s)	Serial numbers of the hardware and software.
System platform	If the problem involves a Mitel application that runs on a PC or server, what is the platform operating system, and what service packs, security software, firewall software, and browser version are installed?
Grounding	What grounding schemes are being employed for all Mitel equipment?
Problem symptoms	Detailed description of the problem symptoms. What is the problem? When did the problem first appear? Have you made any changes to the system programming, hardware configuration or network setup that coincide with the appearance of the problem? Does the problem occur sporadically or only under specific conditions? Try to narrow the scope of the problem down as much as possible. For example, if the system is dropping calls, are only IP Phone to IP Phone calls affected? TDM to TDM calls? IP to TDM calls? or TDM to trunk calls?
Troubleshooting steps	What troubleshooting steps have you taken? Have you been able to eliminate any possible causes of the problem?
Call scenarios	Is the problem occurring between IP to IP devices, IP and remote IP devices, remote IP to IP devices, IP to TDM devices, and so forth?
Network configuration	Do you have a network diagram available? • What is the DHCP configuration and settings in the network? • IP Addressing scheme? • VLAN configuration and settings? • Layer 2 switch configuration and settings • Layer 2 switch port statistics for FCS, collision, and duplex mismatch • Router configuration and settings. Is there a common denominator (router, only one side of subnet, etc.)?
LED status	If hardware, for example a controller or NSU, is affected, what is the status of the LEDs?
	Page 1 of 2

Table 2: Problem Details (continued)

Required Information	Details
Maintenance and software logs	Collect the logs associated with the problem. For example, collect errors on the maintenance port of the NSU. Collect the Alarm log details. On 3300 ICP systems, generate the system diagnostic report. (The PSTSWLOG and XRTC logs are included.) See MKB article 04-1000-00011 for instructions. The Mitel Knowledge Base article explains how to collect specific logs if ESM cannot be accessed.
Phone types	What type of phones are on the system? Is there a specific phone type that is exhibiting the problem? What is the firmware version?
Trunking	What types of trunks (PRI, BRI, LS, DID, XNET/IP, and so forth) are on the system? How are trunk groups set up? How are the LS trunk descriptors programmed?
FAX Support	What type of fax machines are installed? What is their make and model number? Are you using T.38 for faxing? Do the fax calls go over any IP connection, IP trunks or SIP?
Contact telephone number and e-mail address	Be prepared to provide the Mitel Technical Support technician with a telephone number and e-mail address so that the technician can contact you or provide your contact number to other support specialists. If your call concerns an emergency problem, ensure that you can be reached at the telephone number at any time. Don't provide a number that will forward the technician to voice mail. Don't provide a cell phone number that is likely to be unreachable (out-of-range).
	Page 2 of 2

10. If the problem is with an IP Phone, have you collected the following information?

Table 3: IP Phone Information

Question	Answer	Comment
Is there a PC attached to the IP Phone?		If yes, please have the Network Interface Card (NIC) settings of the PC ready. It is recommended that NO power saving options and NO flow control options be enabled.
Have there been broadcast storms?		You can observe a broadcast storm using a packet analyzer (sniffer). A packet analyzer intercepts and logs packet traffic passing over a network.
Is your cabling CAT 5 or better?		CAT 5 or better is recommended for Ethernet connections. Cat 5e is required for 1Gig connections.
Do your L2 or L3 switch statistics show any issues such as Runts, etc.?		Runs/Collision/Frame error may indicate an issue with NIC or a duplex mismatch.
What is the L2 port setting for IP phone and controller?		For IP phones, we recommend access ports that can handle both tagged and untagged packets to and from specific VLANs.
How is the IP phone powered? Power over Ethernet (PoE) or from a power adaptor (transformer) that is plugged into a power outlet.		If powered over Ethernet which L2 PoE switch is being used?
Does your L2 switch have CDP enabled, spanning tree enabled, or Port Fast enabled?		None
What is your speed setting? (10/100, Full/Half, Auto, Fixed?)		None
Do the symptoms improve if the IP phone is set to “auto and lock”?		For controllers, we recommend Access Port. Mitel recommends setting “Auto” on phones. In some unique PC/network, the IP phone may require to hard coding or setting to “auto and lock” mode.
Do the symptoms appear in hands free mode only or do they also occur via the handset?		None
Are you using a headset? What type? What make and model? Is the problem only seen when using the headset?		
Do you have the assert information from the debug (Configuration) menu?		Assert value is saved in the debug mode and reports the last reason that the phone rebooted.
		Page 1 of 2

Table 3: IP Phone Information

Question	Answer	Comment
What type of phones are you using (for example 5330, 5340)? How many display phones are connected to the system? Do any of the phones have PC applications associated with them?		These factors affect system performance.
Is there a pattern? For example, does the problem follow the phone? Can you ping the IP phone?		None.
Have you noted any display information?		None.
Have you tried increasing keepAlives up to 1 minute via the System Administration tool registry entries?		None
Do you have a complex network (for example, multiple nodes and or sites)?		If yes, a network topology diagram is required.
Can you obtain a packet capture via a packet analyzer (sniffer) at the phone level?		Packet capture helps Technical Support to analyze the state of the network and the condition of the phone.
Can you obtain an IP Phone Analysis (IPA) for the phone in question?		IPA provides crucial information about how the phone is reacting.
		Page 2 of 2

Making a Support Call

1. Ensure that you have collected as much information as possible (see Table 2).
2. If possible, establish local or remote access to the system (for example, the 3300 System Administration Tool) that you require support for before you call.
3. Call Mitel Technical Support:
   - From within Canada and the United States, dial the following toll-free number: 1-800-561-0860
   - From outside Canada and the United States, dial the following long-distance number: 1-613-592-7849
4. Describe the nature of the problem to the technician.
5. Record your problem ticket information.

What are Normal Business Hours?

- 8:30 am EST to 5:00 pm LOCAL time (local to North American customer site), Monday to Friday, excluding public holidays.

What are After-Hours Calls?

- Calls originating outside normal business hours (as defined above).

- For example, for customers in the Eastern Time Zone, “after-hours” is defined as 5:00 pm to 8:30 am Monday to Friday, and all day Saturday and Sunday.

CAUTION: Mitel Technical Support will not provide password resets or changes to system options during after-hours support.

Note: After hours calls are charged at a higher rate.

Emergency Calls are Not Charged

If a technician is certified on the current product, phone consultation support is free for emergency calls. However, if a technician is not certified, emergency calls are charged at a higher rate per hour per incident.

The following situations are considered valid emergency calls

- Loss of redundancy in essential environments (see “Definition of Essential Environments” on page 20)
- Loss of essential services (see “Definition of Loss of Essential Services” on page 20)

Note: A Mitel technical support technician will consult their manager if there is a disagreement as to whether a call should be considered an emergency after-hours call.

Definition of Essential Environments

- Hospitals and facilities dedicated to the relief of sickness and suffering
- Emergency response organizations, such as Police, Fire, Ambulance, and Coast Guard
- Defense or military installations
- Penal institutions
- Public utilities such as power or communications facilities

Definition of Loss of Essential Services

- Total system outage
- Total trunk outage
- Greater than 20% of in service system ports are out of service
- Between one and three resets per day

Returning Faulty Hardware

Any Field Replaceable Unit (FRU) that is found to be faulty must be returned with a repair tag containing the following information:

- ❒ The date the device is returned
- ❒ The site where the unit was installed
- ❒ The company name
- ❒ The product name
- ❒ The system serial number
- ❒ The software revision
- ❒ The assembly part number of the item being returned
- ❒ The assembly serial number of the item being returned (this is a white sticker located on the card itself)
- ❒ Any pertinent alarm/error displays. This may include circuit alarm LEDs, console or maintenance error messages, or maintenance log messages.
- ❒ A brief description of the symptoms of the problem.
- ❒ Indicate whether the fault occurred during installation, or while the system was in service.
- ❒ Any further information that may be useful should be included on the rear of the repair tag.

CHAPTER 2

INITIAL SETUP

Initial Setup Troubleshooting Tips

- ☑ Refer to the Technician's Handbook for instructions on how to install and set up a 3300 ICP controller.
- ☑ For hardware related issues, also see See “Controllers” on page 39.

All Controllers

Table 4: General Controller Setup Troubleshooting

Symptom	Possible Cause	Corrective Action
Unable to access the console screen.	You are replacing an existing 3300 ICP controller with another controller, and trying to use the same system IP address for the new controller from a PC on a different subnet.	Initially, you can only connect to the controller from the local subnet. Before you can connect to the new controller from other subnets, you must manually clear the router ARP cache or wait until the router ARP cache is automatically updated. Refer to the latest 3300 ICP Release Notes for instructions.
E2T fails to initialize.	An MXE Server is using the default IP scheme. This causes the E2T of the other controller—which looks to 192.168.1.8 for TFTP on initial bootup—to grab and re-hardcode the IP from the MXE Server.	Do not let the MXE Server use the factory-default IP scheme if there are other controllers with an E2T installed on the same network subnet. At a minimum you need to change the default System IP of 192.168.1.8 to something else that falls within your IP scope.

AX, MXe, CX, or CXi Controller

Table 5: AX, MXe, CX, or CXi Controller Setup Troubleshooting

Symptom	Possible Cause	Corrective Action
Controller not powering up.	Power cable is not securely plugged into the controller and/or power source.	Ensure power cable connections are secure.
	Both power switches on a redundant power supply controller are not on.	Ensure that both power switches are turned on.

Table 5: AX, MXe, CX, or CXi Controller Setup Troubleshooting

Symptom	Possible Cause	Corrective Action
Unable to establish communication with controller via maintenance PC	Controller has not finished starting up.	The controller can take up to 15 minutes to start up.
	PC communication application (for example VT 100 emulator program) serial port settings incorrect.	See “Connect to PC” in the “Initial Setup” chapter of the *MCD Technician’s Handbook* for correct settings.
	Crossover Ethernet cable used to PC to controller.	Use a straight-through Ethernet cable.
	PC Network Interface Card IP address not programmed.	Program the PC’s NIC with the following settings: • IP Address: **192.168.1.n** (where n is a value between 30 and 254) • Subnet Mask: **255.255.255.0**
	Maintenance PC on different subnet.	Configure maintenance PC on same the same subnet as controller.
	IP address and subnet mask for RTC entered incorrectly.	Enter IP addresses without leading zeros. For example, 192.168.1.2; not 192.168.001.002
E2T does not come up even though **inet on ethernet** is programmed and the flag is set to 0x40.	ET2 was hard coded with an IP address and then later changed to request an IP address from the DHCP server. This change is made by changing the **flags (f)** parameter in the bootline of the E2T from **0x0** (hardcode) to **0x40** (DHCP). If **any** IP addresses remain on the E2T (at “inet on ethernet”, “host inet” or “gateway inet”), the E2T will use them and will obtain the rest of its parameters from the DHCP server.	When changing the flag from 0x0 to 0x40 on E2T, ensure that you blank out ALL IP addresses in the bootline of E2T. Refer to “Programming the E2T via a Debug Cable or Secure Telnet” in the *MCD Technician’s Handbook*.
	RTC is set up with a different virtual LAN (vlan).	From the RTC shell, remove the vlan using the **cv** command:
When adding subnets to the internal DHCP server you receive the error message “No more room for records”.	Number of available subnets exceeded.	Refer to Mitel Knowledge Base article 06-5157-00008 for details.
After a new install, the internal DHCP server is not supplying addresses to IP devices.	Internal DHCP server is not activated.	The internal DHCP server is not activated by default. If your system relies on the internal DHCP server, you must turn the flag on by issuing the **DBMS SAVE** command.

Table 5: AX, MXe, CX, or CXi Controller Setup Troubleshooting

Symptom	Possible Cause	Corrective Action
Issuing the **close** command during a secure Telnet session to the RTC results in an error message.	When you issue the **close** command inside Telnet, the Telnet shell interprets it as a close(0) command and sends it to VxWorks.	Refer to Mitel Knowledge Base article 04-3849-00290.
After installing 80 GB SATA hard drive with pre-loaded software of 10.1.2.16 for CX II or CX(i) II, 3300 can load up successfully, but you cannot access ESM.	80 GB SATA hard drive for CX II or CX(i) II which is pre-loaded in the factory has vlan 206 pre-configured. As a result, PC on the native vlan cannot access ESM form etc after installation. The part number affected is 50006294.	Refer to Mitel Knowledge Base article 10-5191-00192.
CXi II alarms show FAN alarm with 100% failure.	The fans are working, but the controller thinks they are faulty because CXi II uses quieter fans,	Upgrade to at least MCD Release 4.1 or later. This feature change was also delivered in MCD Release 4.0 SP3. Refer to Mitel Knowledge Base article 11-6052-00011.

MXe Server Setup

Table 6: General Setup Troubleshooting

Symptom	Possible Cause	Corrective Action
Cannot access the Server manager over IP connection.	Communication application (for example, Hyperterminal) connection parameters set incorrectly.	See the table “Communication Connection Parameters” in the “Initial Setup” chapter of the *MCD Technician’s Handbook* for the correct settings.
No RS232 connection to the printer port.	MXe Server has not yet enabled the printer ports.	Ensure that you wait 3 minutes before attempting to connect. The MXe Server takes approximately 3 minutes before the software enables the printer port.
Unable to access the Server Console screen on the MXe Server.	The MXe Server and the PC are in a different subnet, and MSL has not been configured to allow traffic from the subnet.	Configure MSL to allow traffic from the subnet.
Unable to access Server Manager screen over the IP network with IE.	Crossover Ethernet cable used to connect PC Network Interface Card to controller	Use a straight-through Ethernet cable.
	NIC IP address not set correctly.	If the system is still using the default IP configuration, set the NIC IP address to 192.168.1.20.
Unable to login to Managed Application Server Manager application.	Using wrong password.	You must enter the Linux admin password that you set through the Server Console. If you have lost the MSP "root" password, the only way to recover is to reinstall MSL.
Unable to access system from MCD Software Installer or other tools such as Enterprise Manager, or System Administration Tool client stations.	Tools reside on different network.	Add the network through the Server Manager. Under Security, click Local Networks and add the Network IP Address, Subnet Mask, and Router IP Address.
Unable to set system date and time for the system tools.	The Managed Application Server application date and time setting does not apply to the.3300 ICP.	Set the system date and time from the Group Administration Tool.

Licensing

For general AMC troubleshooting, also see the AMC Troubleshooting Guide.Refer to Mitel Knowledge Base Article 11-5191-00211.

Table 7: Troubleshooting Licensing and Optioning

Symptom	Possible Cause	Corrective Action
License and Option Selection error.	The System ID or i-Button has not been installed.	Install the SysID module or i-Button. Note that the MXe Server does not have a SysID module or an i-Button. If you still can't fix the problem, call Technical Support. Make sure you have the following information on hand before calling: • The controller's VxWorks parameters (boot device, host file, inet on ethernet, host IP address). • The error message(s) in the RTC shell.
Unable to communicate with the Application Management Center (AMC).	• Inability to communicate with the AMC because unable to find the AMC servers via a DNS lookup. • Inability to communicate with the AMC because of network/system configuration. • Inability to communicate with the AMC using specific protocols or ports due to router or firewall configuration	Refer to Mitel Knowledge Base Article 11-5191-00211.
Cannot move licenses after manual upgrade.	There is a specific procedure that you must follow to move licenses after a manual upgrade.	Refer to Mitel Knowledge Base Article 06-9999-00013.

Table 7: Troubleshooting Licensing and Optioning

Symptom	Possible Cause	Corrective Action
You receive an e-mail that indicates that the evaluation period for the Management Access Point (MAP) will expire soon. Sample e-mail output from Management Access Point related to 3300: Message 12345 from Mitel_7100 Date: 02/07/05 Time: 17:01:36 Type: 1 SubType: 300 Description: License reminder Data: Application m3300snmp.app - Evaluation period expires in 2 day(s)	If the activation key was not entered on the Management Access Point (MAP) during installation, a license reminder e-mail is sent from the Management Access Point to remind you that the evaluation period will soon expire. Note: This condition does not cause any service outage on the 3300 ICP. The e-mail is just a reminder that the Management Access Point does not have the proper key activation code.	Install the Management Access Point with the proper key activation code.
The system is generating “Warning” license violation messages in maintenance logs and the ESM System Administration Tool (pop-ups and banner status messages).	One of the following warning-level license violation events has occurred: • Over Allocation • Missing DLM • Missing Application Group Member • Core Package capability exceeded • License Keys cannot be validated • System ID mismatch • SDS is off • Duplicate System • Multiple DLMs • Failure of timely synchronization with AMC • Application Group is in license violation mode • “licensekeys” or “licensecert” file is corrupt or has been tampered with	Correct the license violation event.
The system is generating “Minor” license violation messages in maintenance logs, alarms, and the ESM interface (pop-ups on multiple forms and banner status messages).	The “Warning” level license violation escalation timer has expired (15 days after the original event).	Correct the license violation event.

Table 7: Troubleshooting Licensing and Optioning

Symptom	Possible Cause	Corrective Action
The system is generating “Major” license violation messages in maintenance logs, alarms, and the ESM interface (pop-ups on multiple forms and banner status messages).	The “Minor” level license violation escalation timer has expired (20 days after the original event) OR An attempt has been made to over-allocate a license that cannot be over-allocate (e.g. an ACD Active Agent license).	Correct the license violation event.
The system is generating “Critical” license violation messages in maintenance logs, alarms, the ESM interface (pop-ups on multiple forms and banner status messages), the Desktop Tool, and device displays.	The “Major” level license violation escalation timer has expired (25 days after the original event).	Correct the license violation event.
The system has reached “System Lock” license violation level and is generating a variety of error messages and alarms. In addition, the Desktop Tool is disabled and all sets except attendant consoles are placed in restricted service mode. Users can place emergency and attendant calls, and receive calls, but they cannot place regular outgoing calls.	The system is locked when an over-allocation violation is left uncorrected. For this to happen, the “Major” level license violation escalation time must expire (30 days after the original event) and the number of licenses that have been over-allocated must exceed 5% of all purchased licenses.	Correct the license violation event.

CHAPTER 3

HARDWARE

Hardware Troubleshooting Tips

- ☑ Only change one setting at a time (either a hardware or software setting).
- ☑ Observe carefully and document all observations (for example, feature programming, call states, time of day, problem symptoms and so forth).
- ☑ If all the functionality supported by a module or card is out of service, it is likely defective. If possible, swap the module or card with a known working module or card to confirm.
- ☑ Check the Alarm logs in the System Administration tool for hardware alarms.
- ☑ Check the LEDs on the hardware. Refer to “Appendix D: Status LEDs” in the *MCD Technician’s Handbook* for LED state information.
- ☑ Verify that the IP addresses reserved for the hardware units are not used elsewhere on the system. See the “Installation Planner” chapter in the *MCD Technician’s Handbook* for a list of the IP addresses that are reserved for the Analog Main Board (AMB) and the CIMs on the ASU and ASU IIs.
- ☑ For phone related issues, is the problem occurring
  - on a single phone?
  - on a group of phones of a specific type (for example IP Phones only)?
  - on a group of phones within a specific Class of Service only (indicates a potential programming conflict in COS Options form)?
  - during local-to-local calls only or local-to-external calls only?
- ☑ For phone or trunk related issues, if you don’t find the solution in this chapter, you should also check the troubleshooting tables in
  - Chapter 5: “System Features” on page 95
  - Chapter 6: “Trunking” on page 113
- ☑ Use the IP Phone Analyzer Tool to help you troubleshoot IP phone problems
- ☑ In the System Administration Tool use the following Maintenance and Diagnostic forms:
  - *Hardware Compute* form: displays details of the Real Time Controller (RTC) card and Ethernet-to-TDM (E2T) card
  - *Hardware Modules* form: displays the Mitel Mezzanine Card (MMC) modules that are installed in the system.
  - *IP Telephone forms*: displays all IP phones in the system and their status.
- ☑ For help with *diagnosing* hardware problems, see “Hardware” on page 211.
- ☑ For help with *diagnosing* phone hardware problems, see “Phones” on page 191.

Hardware Alarms

Table 8: Hardware Alarms Troubleshooting

Alarm	Probable Cause	Corrective Action
ICP Comms	E2T card has no IP address.	**If you are using the controller's internal DHCP server for the E2T**: ensure you assigned a static IP address to the E2T using the correct MAC address (see "Configure the Layer 2 Switch" in the "Initial Setup" chapter or the *MCD Technician's Handbook* for instructions). **If you are using an external DHCP server for the system:** verify that options are programmed correctly (see "Configuring External DHCP Settings for E2T" in the "Installation Planner" chapter of the *MCD Technician's Handbook* for instructions).
	DHCP is corrupted.	Rebuild the DHCP scope. if DHCP is not running, start by doing a dbms save.
	Incorrectly programmed E2T IP address or incorrect setup of debug cable.	Verify that E2T VxWorks parameters are correct (see "Programming E2T via Debug Cable or Secure Telnet" section of the *MCD Technician's Handbook* for instructions).
	RTC is set up with a different virtual LAN (vlan).	From the RTC shell, remove the VLAN using the **cv** command. You may also have to remove the VLAN on the E2T. The process is the same, but you do it from the E2T VxWorks shell.
	If the alarm is occurring on a CX/CXi controller that is running pre- 3300 release 9.0 UR2 software, it is a false alarm.	To clear the alarm without a reboot: 1. From the RTC shell enter the following -> lkup "ClearAlarm" 2. This command Identifies the Hex code associated with the ClearAlarm. Note that this code is software load dependent. The system response will be similar to the following: ClearAlarm (void) 0x0033763c text <======= this is what I need LicenseManagerImpl : : ClearAlarm(void) 0x00fc99ac text ClearAlarm 0x001136c8 text value = 0 = 0x0 3. Enter the ClearAlarm(void) hex code. For example: --> 0x0033763c( )
	E2T card is defective.	Check the Hardware Compute Cards form in the System Administration Tool. If the IP Address for Slot 2 displays "Not Responding", replace the E2T card.

Table 8: Hardware Alarms Troubleshooting

Alarm	Probable Cause	Corrective Action
Media Gateway (MG) Comms (MXe Server only)	IP configuration is incorrect or duplicated	Check that the IP addresses are correct by checking the System IP Properties form on the System Administration Tool.
	RTC (Media Gateway) card has no IP address.	Refer to Mitel Knowledge Base article 09-5157-00026 for instructions on how to set the IP address.
DSP Status	A percentage of DSP resources are unavailable. The failure of one or more, but not all, DSPs results in a Minor alarm. Critical alarm indicates that all DSPs have failed. In the event of an alarm, reset the system as soon as possible. If the DSP continues to fail, replace the module.	Use the **Show Status DSP** maintenance command to identify status of DSPs in the controller. Install required DSP modules. See “Increasing DSP Resources” in the “Installation Planner” chapter of the *MCD Technician’s Handbook* for instructions.
	DSP licenses are enabled but not enough DSP resources are available to support compression requirements	Install required DSP modules. See “Increasing DSP Resources” in the Installation Planner chapter of the *MCD Technician’s Handbook* for instructions.
	Faulty circuit on DSP module	Replace DSP module.
DSP Card Status	DSP card is defective.	For a defective DSP module, ensure that the module is seated securely. For an embedded DSP failure, replace the controller. Use **Show Status DSP to identify the location of the defective module.**
Fan	Fan is defective (AX/MXe/MXe Server).	Replace the fan (see Note below).
Fan	The fans are working, but the controller thinks they are faulty because CXi II uses quieter fans,	Upgrade to at least MCD Release 4.1 or later. This feature change was also delivered in MCD Release 4.0 SP3. Refer to Mitel Knowledge Base article 11-6052-00011.
One PSU	Power supply unit is defective (AX/MXe/MXe Server).	Replace the PSU (see Note below).
Two PSU	Power supply unit is defective (AX/MXe/MXe Server).	Replace the PSU (see Note below).
RAID Hard Disk	Hard disk has a fault (MXe/MXe Server).	If the alarm occurs on the primary drive, replace the hard disk (see Note below). Refer to Mitel Knowledge Base article 06-2806-00012 and KB11-5191-00213. If the alarm occurs on the secondary drive, check the primary drive for faults. (In some cases, the primary drive has a sector error while the secondary drive is fault free.)

Page 2 of 3

Table 8: Hardware Alarms Troubleshooting

Alarm	Probable Cause	Corrective Action
Receivers	An active DTMF receiver circuits on the active Peripheral Switch Matrix card has a fault. By default all 3300 ICPs are assigned three DTMF receivers, each having 16 circuits for a total of 48 circuits.	Replace Peripheral Switch Controller.
TDM Clock	Stratum 3 clock module in controller has failed.	Replace Stratum 3 clock module.
Temperature	Temperature in the system is getting too high.	System has overheated. Cool down system to clear alarm. This alarm applies to the MXe controller, MXe Server, CX/CXi controllers, and AX controller only.
SFT Zones	System Fail Transfer zones have switched into SFT mode.	Determine cause for switch to SFT mode.
SYSID Mismatch	The System Identification module or i-button is not installed or is incorrect.	Install or replace System Identification module or i-button.
Note: Enter the **Show Status Redundant** maintenance command to identified the failed component. A minor Fan, Power Supply, or RAID alarm in the MXe or MXe Server means that only one of the components has failed. A major alarm means that more than one component has failed. See the *MCD Technician's Handbook* for hardware replacement procedures.		
Page 3 of 3		

Controllers

MXe Controller

Table 9: MXe Controller Troubleshooting

Symptom	Probable Cause	Corrective Action
E2T fails to initialize.	Changing from a hard coded E2T IP address to requesting one from the DHCP server. (If **any** IP addresses remain on the E2T (at “inet on ethernet”, “host inet”, or “gateway inet”), the E2T will use them and will obtain the rest of its parameters from the DHCP server.)	For information and guidance for correcting this problem, refer to "Programming E2T via Debug Cable or Secure Telnet" in the *MCD Technician’s Handbook*.
	RTC is set up with a different virtual LAN (vlan).	From the RTC shell or the E2T VxWorks shell, remove the vlan using the **cv** command.
	E2T card defective.	Check the Hardware Compute Cards form in the System Administration Tool. If the IP Address for Slot 2 displays “Not Responding”, replace the E2T card.
Unable to communicate with MXe	You are attempting to use port 2 to access the MXe controller but the Layer 2 IP address is not programmed.	Use port 1 to access the MXe controller. Then launch the System Administration Tool and program the Layer 2 IP address.
Soft fault reported intermittently by RAID controller.	Soft fault comes indirectly from the hard drive itself.	Refer to Mitel Knowledge Base article 06-2806-00012.
Audio problems from IP to IP or IP to TDM.	E2T is unable to communicate with devices off its subnet.	If the problem is IP -> IP or IP -> TDM: Check the default gateway on all components involved in the call that is having audio problems. For example, you might see this issue when the following pairs are on different subnets: • E2T to E2t • E2t to IP phone • IP phone to IP phone

CX/CXi Controller

Symptom	Probable Cause	Corrective Action
Unable to connect to the controller over the IP network to ESM.	Database being used is from a system that had dual-VLANs enabled, so the management PC, untagged on VLAN 1, cannot reach the controller on the Voice VLAN.	Hard code the PC onto the same subnet as the 3300 ICP you are connecting to.
IP Phones on third-party Layer 2 switch cannot connect with the CXi.	System has VLAN enabled but the “tagging” is being removed prior to connecting with Port 17.	The CXi must receive VLAN tags (if VLAN enabled) to allow an IP phone to connect with the CXi. Connect the third-party switch to the 3300 ICP using a VLAN-enabled trunk port. Then use the third-party L2 switch to pass the Q and P tags to Port 17.
Unable to connect to the DSL modem.	Bad connection, incorrect password, incorrect username, or wrong protocol.	Review Maintenance Logs for: • Wan_port: state=down, • proto=pppoe, cause=wan=start. Review ISP information sheet and make sure that the username, pw and protocol are correct. Disable and Enable the WAN Access in Internet Gateway/Wan Settings.
CXi ports 1-16 not functioning.	Layer 2 port IP Address is not programmed.	Ensure IP Network Configuration is programmed properly.
Connection failures: ISP, IP trunks, or IP phones.	Network configuration programming problem.	Verify programming in the following forms: 1. System IP Properties The address cannot conflict with the L2 Switch IP Address, and it must be on a different subnet than the WAN Ethernet IP Address. 2. Layer 2 Switch form To program global settings and configure the Ethernet ports for the Layer 2 switch. 3. IP Routing form Lists routes to destination networks on the LAN. 4. WAN Settings form To enable the WAN interface and provide internet connectivity settings for Static IP, DHCP, or PPPoE. 5. Remote Access (PPTP) form 6. Firewall Control form 7. Port Forward Table form
		Page 1 of 2

Symptom	Probable Cause	Corrective Action
Not routing IP traffic correctly.	Default Gateway should be third-party router (if one is installed), otherwise L2 IP Address should equal Gateway.	IP Routing form indicates a network list. All subnets referenced on this network list will follow the default gateway, otherwise the route will be directed to the WAN port (ensure that it is enabled).
No power on CXi ports 1-16.	Device is pulling too much power; power is disabled in programming; 100 Watt budget has been exceeded.	Refer to Engineering Guidelines, Mitel IP Phone Power. When power budget is exceeded ports will shut down from port 16 to port 1. Run the **L2 Poestatus** maintenance command. Check Layer 2 Switch programming. Check device for fault.
Connection failures: IP trunks.	IP trunks cannot work through the WAN port.	Install a third-party router (default gateway) and disable the WAN port OR install a third-party router (default gateway), change Network list to include routes that will follow default gateway and enable WAN port. **Note**: IP trunk will follow default gateway (3rd party router).
CXi II alarms show FAN alarm with 100% failure.	The fans are working, but the controller thinks they are faulty because CXi II uses quieter fans,	Upgrade to at least MCD Release 4.1 or later. This feature change was also delivered in MCD Release 4.0 SP3. Refer to Mitel Knowledge Base article 11-6052-00011.
		Page 2 of 2

MXe Server

Table 10: MXe Server

Symptom	Probable Cause	Corrective Action
New MXe fails to boot after drive is mirrored. “Error auto-loading file: errno = 0x850001”	The firmware being shipped on the RTC flash is not the current version.	Reinstall the software to update the RTC to the proper load. OR Issue the **UpgradeBootrom ALL** maintenance command from the System Administration Tool.
		Page 1 of 3

Table 10: MXe Server

Symptom	Probable Cause	Corrective Action
Suspected APC failure.	The APC is faulty, or the APC battery is low.	Remove and replace the APC-MXe battery. See the “Application Processor Card” section in the “Install and Replace Units” chapter of the *MCD Technician’s Handbook* for instructions. If that doesn’t fix the problem, ping the APC IP (System IP) address. If the ping is successful, ssh to the APC IP address and type a few basic commands like: >ll >ls >cd If these commands succeed, the problem is likely not the APC.
Ping to APC failed.	APC is faulty.	Remove and replace the APC-MXe battery. See the “Application Processor Card” section in the “Install and Replace Units” chapter of the *MCD Technician’s Handbook* for instructions. If that doesn’t fix the problem, make a serial connection to the printer port (38400 8N1). <Enter> to login to Linux, and issue some basic commands: >ll >ls >cd If these commands succeed, APC is not faulty. See Network connectivity is broken, below.
	Network connectivity is broken.	Recheck network connections.
Login via the serial connection to printer port fails	Either the cable is not connected properly, or there is a problem with the application you are using to connect.	Check the cables. Try the basic connection options: Vt100 terminal running 38400 8N1, and so on. If that does not resolve the problem, power down the fulll unit and power it back on. If there is not output and no MSL login, then you will have to consider replacing the APC. Given the effort required to replace the APC, you may choose to replace the full system.
		Page 2 of 3

Table 10: MXe Server

Symptom	Probable Cause	Corrective Action
“Operating System not found”: No operating system image has been found on the hard disk.	Installation error.	Reinstall the software.
	RAID Controller is faulty.	Replace the RAID controller. See the “MXe/MXe Server RAID Controller” section in the “Install and Replace Units” chapter of the *MCD Technician’s Handbook*.
	Hard disk has crashed.	Replace the hard drive. Refer to the “Install and Replace Units” chapter of the *MCD Technician’s Handbook*.
“GRUB loading...”	Problem with the Hard drive master boot record.	Reformat the hard drive. If this does not solve the problem, replace the hard drive using the instructions in the “Install and Replace Units” chapter of the *MCD Technician’s Handbook*.
		Page 3 of 3

Service Units

Table 11: Service Unit Troubleshooting

Symptom	Probable Cause	Corrective Action
Network Service Units		
NSU not functioning correctly.	Issue with external equipment.	Check external equipment.
	Faulty fiber connection between NSU and controller.	Fix the fiber connection, and ensure that the LEDs of both FIMs are solid green.
	Programming error.	Check the programming in the following forms: • MSDN/DPNSS/DASS2 Trunk Circuit Descriptor Assignment • Miscellaneous Assignment (for NSU-BRI only) • Link Descriptor Assignment.
NSU fails to come up after upgrade or new installation (Both the red and amber LEDs, or just the amber LED, are alternating between L0/L1).	Automatic NSU upgrade is in progress.	Wait 15–20 minutes for the NSU upgrade to complete. **CAUTION: Do not power down when the amber LED is alternating between L0/L1. Powering down the NSU may corrupt the NSU software.**
The LEDs are flashing green and amber for more than 30 minutes during an NSU upgrade.	Corrupted NSU software.	Refer to Technical Bulletin 58004932 for information on flashing the NSU.
NSU fails to come up after upgrade or new installation. NSU continues to reset on a regular interval and/or the LEDs on L0 and L1 continue in alternating flash cycle longer than 30 minutes.	NSU flash is corrupted.	Refer to Mitel Knowledge Base article 04-1000-00026_2 for instructions.
NSU fails to load after upgrade or install with “Unexpected database error”	Database version is unsupported (incompatible).	Refer to Mitel Knowledge Base article 04-5115-00002 for instructions.
NSU or PRI card fail to load after upgrade or database restore.	NSU and PRI cards fail to load because the database version does not match the current software load on the card.	Refer to Mitel Knowledge Base article 05-5173-00022
NSU keeps resetting with **no IMAT db** error message.	No IMAT database is saved to the NSU (PRI/QSIG).	Use IMAT to save the corresponding database to NSU (PRI/QSIG).

Page 1 of 3

Table 11: Service Unit Troubleshooting

Symptom	Probable Cause	Corrective Action
After changing NSU from T1 to E1, NSU remains unassigned.	NSU does not reflash.	• Flash the NSU (refer to Technical Bulletin 58004932) *OR* • Delete datetag.txt via ftp *OR* • From the debug terminal, issue force dl for the NSU.
NSU fails to boot, with an error message. Boot line timeout.	Universal NSU programming is not complete.	1. Ensure that the NSU is programmed as a Universal T1 or E1 (not T1 or CEPT). 2. Program the proper link descriptor with the proper integrated access, and assign to the corresponding NSU unit (for example: ISDN node for PRI protocol, T1D4 for T1D4, DPNSS for MSDN). 3. Program at least one trunk.
PRI/QSIG NSU fails to boot.	Database not compatible with new load.	1. Connect IMAT to the PRI NSU and start IMAT. 2. Download the database from the NSU to IMAT. 3. Save the database from IMAT to the NSU. 4. A message appears asking if you want to convert the database. Select **Yes**. 5. When the database has finished saving, reset the NSU.
Unable to FTP into the NSU.	Release 4.1 and later requires a username and password to login.	Enter: username, **mitel** password, **passwd1**
NSU is up, but L0 or L1 LED is solid red.	No physical connection to far end.	1. Verify and fix wiring. 2. Check DIP Switch 6. If it is UP, set it to DOWN to see if this makes any difference (see “Universal and R2 NSU DIP Switch Settings” in the “Hardware Reference” chapter of the *MCD Technician’s Handbook*).
NSU is up, but L0 or L1 LED is flashing green.	Layer 2 protocol mismatch.	Change protocol through IMAT
Distorted voice or loud noise on NSU trunks.	Voice encoding is not set properly.	Change Voice encoding in the link descriptor to **invert** for **T1**, and **ADI invert** for **CEPT** (this does not apply to Embedded PRI). Set termination impedance switch correctly (75 ohms or 120 ohms).

Page 2 of 3

Table 11: Service Unit Troubleshooting

Symptom	Probable Cause	Corrective Action
Unable to connect to NSU trunks	No fiber connection between the controller and NSU.	Fix the fiber connection, and ensure that the LEDs of both FIMs are solid green.
	Universal NSU programming is not complete.	1. Ensure that the NSU is programmed as a Universal T1 or E1 (not T1 or CEPT). 2. Program the proper link descriptor with the proper integrated access, and assign to the corresponding NSU unit (for example: ISDN node for PRI protocol, T1D4 for T1D4, DPNSS for MSDN). 3. Program at least one trunk.
Layer 2 is down.	Layer 2 protocol mismatch.	Check your IMAT database and verify with your Telco which protocol you should use.
IMAT fails to collect database files from the NSU.	When using IMAT to retrieve the database from the Universal NSU the database files do not appear to have been downloaded. The IMAT application simply does not provide information to identify success or failure to download the database. At the bottom left hand corner of the IMAT application, you will see “please select a menu option”. The maintenance logs can be downloaded, you will get the IMAT indication that the maintenance logs have been received.	Ensure that the NSU is actually running as ISDN node in the link descriptor under the integrated digital access field. If it is not, there are no DBA files, which represent the IMAT database. Maintenance logs are maintained on NSUs, which is why they can be downloaded**.**
Analog Service Unit		
User can hear clicking sound while on a call on an external ASU ONS circuits.	Message Waiting voltage cycling.	Refer to Mitel Knowledge Base article 05-4409-00008.
Voice calls on ASU have an echo.	Faulty programming.	Ensure that the **ARS Call Progress Tone Detection form** for the analogue trunks is programmed correctly and ensure that the **Tone to Detect** entry is left blank (i.e. no tone to detect). If the **Tone To Detect** entry is set to detect a tone, it may cause echo.
		Page 3 of 3

Gateways

Table 12: Gateway Troubleshooting

Symptom	Probable Cause	Corrective Action
CITELlink Gateway issues.	Refer to Mitel Knowledge Base article 04-3849-00016 for possible causes.	Refer to Mitel Knowledge Base article 04-3849-00016 for corrective actions.
Unable to configure the AudioCodes Mediant 1000 gateway for SIP Lineside with the 3300 ICP	Configuration issues	Refer to Mitel Knowledge Base article 08-5159-00005 for configuration details.

Peripheral Cabinets

Table 13: Peripheral Cabinet Troubleshooting

Symptom	Probable Cause	Corrective Action
Peripheral Cabinets		
ONS sets not ringing on peripheral node, however set can be answered and a two-way conversation carried out.	Frequency-Switch Keying (FSK) is not assigned in the Peripheral Switch Controller/Digital Signal Process or Assignment form, and the ONS sets have COS CLASS/CLIP option enabled.	1. Assign FSKs, or 2. Turn off ONS CLASS/CLIP in the ONS Class of Service.
		Page 1 of 3

Table 13: Peripheral Cabinet Troubleshooting

Symptom	Probable Cause	Corrective Action
You have migrated a peripheral or DSU cabinet from an SX-2000 system to a 3300 ICP system and the Cabinet does not boot up.	Incompatible FIM modules.	Before you migrate a PER/DSU to a 3300 ICP, ensure that you identify the types of FIM modules required before migrating: • single to single • multi-mode (820 nm) to multi-mode (820 nm), or • multi-mode (1300 nm) to multi-mode (1300 nm). The part numbers for the supported FIM modules are listed in the “Install and Replace Units” chapter of the *MCD Technician’s Handbook*.
	LS/GS Trunks.	Ensure that the programming matches the CO trunk equipment configuration (if the CO equipment is loop start, ensure that the trunk circuit is programmed as loop start) and that the system option “Interconnect Checking for Conference Calls” is enabled in the System Options form to prevent “hung-up” trunks. Check Tip and Ring polarity. Check Tip and Ring voltages.
	Insufficient DTMF receivers (not enough for peak traffic load).	Add DTMF resources.
	Fault in peripheral switch control.	Swap the following cards with known working cards: • Peripheral switch controller card (slot 16 of a peripheral cabinet) • Peripheral Resource card • Control Resource card (SX-2000 MicroLIGHT systems only)
Faulty LS/GS Trunk Card, E&M Trunk Card, or DID/Loop-Tie Trunk Card.	Faulty external trunk equipment or main distribution frame connections	Fix external trunk equipment and check main distribution frame connections.
	Faulty main distribution frame and system connections.	Check main distribution frame and system connections.
	Faulty programming.	Check programming. See the System Administration Tool online help for details.
		Page 2 of 3

Table 13: Peripheral Cabinet Troubleshooting

Symptom	Probable Cause	Corrective Action
DSU Cabinet		
Microlight DSU cabinet connected to a 3300 ICP via Triple FIM -circuits 2 and 3 is not functioning.	Microlight Peripheral Cabinet ia not installed and connected to Triple FIM -circuit 1.	If you connect a Microlight DSU cabinet to the 3300 ICP via Triple FIM circuits 2 and 3, you must ensure that the Microlight Peripheral Cabinet is connected to Triple FIM circuit 1. Triple FIM circuit 1 provides the clock source for all Triple FIM circuits. Without circuit 1, there is no clock source for other FIM circuits (2 and 3), resulting in the internal DSU not working. Also ensure that the Control Resource Card (CRC) has not been removed from the MicroLight cabinet.
Faulty PRI or BRI Card.	Check external equipment and connections.	Fix connections or replace cabling.
	The connections between the interface assembly and the interface card.	Fix connections.
	Faulty backplane cable connections (or bent pins on backplane and inside shelf).	Replace cable or straighten pins on backplane.
	Faulty programming.	Check programming. Refer to the System Administration Tool online help.
	Faulty Interface Assembly.	Replace Interface Assembly.
	Defective card.	Replace card.
Unable to establish a connection between the IMAT PC and the PRI or R2 card.	Faulty Dial-Up Networking connection settings.	Check the Dial-Up Networking connection settings.
Unable to fully insert a Triple FIM card (Part Number 50001856) into the control slot of Microlight cabinet. or connect the Triple FIM to the backplane.	The plastic tabs (stopper) were improperly installed on the cards. by the manufacturer preventing proper installation.	Refer to Mitel Knowledge Base Article 08-5191-00105 for a solution.
		Page 3 of 3

Embedded Modules

Table 14: Embedded Module Troubleshooting

Hardware	Symptom	Probable Cause	Corrective Action
Embedded PRI Module.	Embedded PRI Module fails to initialize. The LEDs on the embedded PRI (Framer) module are off. The trunks for the module are unassigned.	Module has failed to initialize because the link descriptor is not programmed correctly.	Check the programming for the link descriptor that is assigned to the embedded PRI (Framer) module: For T1 only: • B8ZS Zero Code Suppression: Yes • Operation Mode: DSX-1 or CSU • CSU Tx Line Build-Out (dB.): This T1 parameter ensures reliable operation of the network. Select from 0, 7.5, 15, or 22.5 dB. Your carrier can advise you of the correct setting. The default is 0 dB. • DSX-1 Line Length (Ft.): 0-133 feet. • Extended Super Frame: No • Inverted D channel (DPNSS only): Yes For E1 only: • CRC-4 Enabled: “No” in North America; “Yes” in Europe • E1 Line Length (Ft.): 0-133 • E1 Impedance (Ohms): 120 **Note:** For E1 only, 90% of E1 service providers in Europe require that you set the “CRC-4-Enabled” option to “Yes”. Please consult with your service providers for proper settings. **Note:** For DASS/DPNSS (E1), set the “CRC-4 Enabled” option to “No”.
			Page 1 of 3

Table 14: Embedded Module Troubleshooting

Hardware	Symptom	Probable Cause	Corrective Action
Dual Framer (T1/E1) Module	After installing a Dual Framer (T1/E) module and programming a Digital Link Descriptor in the Digital Links form, the Framer module LED appears red. If you perform the STAT 7 1 2 maintenance command, the PLID shows “No card installed at requested slot”. (A loopback connector (Pins 1,2 to 4,5) will cause the LED to flash green.)	Protocol type not programmed.	After a digital link has been programmed, you must use the ISDN Protocol form to program the protocol type. System Configuration > Trunks > Digital Trunks > ISDN-PRI > T1 > Protocol Assignment As soon as a protocol is assigned a STAT of the card will show a valid state such as “not seizable”, or “idle”.
DSP card or module	Card fails to come out of reset.	Both PostSoftware and PostMaintenance logs are generated as well as a “DSP Card Status” alarm.	Disconnect controller power and then reconnect. Newer versions of DSPs have been updated to prevent this issue from occurring.
	DSP Fails to Boot.	No DSP resources. No dial tone on analog devices, embedded voice mail ports don't function, and so forth.	Remove and re-seat the card. Reboot. They should be looking at the connectors for bent pins etc. NOTE: Ensure that the screws are not over tightened! Over tightening of one side can cause the other side connector to rise up.
		PostSoftware Log: StartUp (BindId=0) pCOam->coDspBoot failed with: DSP_PROGRAM_ERROR for card: 3 and dsp: 0	If the problem persists, then remove/replace the card completely. This card only needs to be immediately replaced if it is the only card/dsps being used for Telephony. If it was being used for Telephony, but there are still dsps left in the system, this is still fine but the user may be traffic limited until it is replaced.

Table 14: Embedded Module Troubleshooting

Hardware	Symptom	Probable Cause	Corrective Action
DSP card or module.	DSP Run-Time Access Fault.	These are mostly exceptions that either produce an XRTC file or simply perform a hard reset on the system. These can occur at any point after the card has been taken out of reset but are considered separate from the Booting Process.	If the system is stuck in a reboot sequence. Remove and re-seat the card. Reboot. They should be looking at the connectors for bent pins etc. NOTE: Ensure that the screws are not over tightened! Over tightening of one side can cause the other side connector to rise up. Obtain System Diagnostics Reporting output, or at a minimum, the XRTC and PostSoftware logs.
	DSP Overflow Error.	As of 3300 Release 7.0, these are now tracked and monitored by the DSP Service Provider. If these occur, the dsp will be taken out of service and a “DSP Status” alarm is raised.	If this happens, and it is a HW problem, it should be repeatable. Remove and re-seat the card. Reboot. Look at the connectors for bent pins etc. NOTE: Ensure that the screws are not over tightened! Over tightening of one side can cause the other side connector to rise up.
		Prior to 3300 Release 7.0, these were only reported as PostSoftware Log: RsrcAlloc() failed with result DSP_OVERFLOW.	If it is a pre R7.0 system: From the RTC shell, enter: DumpCaps (x,y) where x is the card number and y is the dsp number reported in the PostSoftware Log. Capture these results and send them to Mitel Product Support. Obtain System Diagnostics Reporting output file and contact Mitel Product Support.
			Page 3 of 3

Phones

Note: IP phone troubleshooting tips also apply to the 5540 IP Console.

General Phone Issues

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
Any	No calls are being received.	Programming error.	Check the • programming to make sure the calls are not forwarded or rerouted elsewhere automatically by the system. • Class of Service Options Assignment to make sure the programming allows incoming calls.
Any	Dial Tone at the set but user is unable to make calls	Programming in Class of Service or Class of Restriction forms are preventing calls	Check the following: • Establish if the extension being used is the one assigned to the user. • Establish the type of calls the user is trying to make. • Check the programming on the system for that extension. Look at the Class of Service and Class of Restriction Assignment in particular • Check to see if the number dialed is using a route list or plan. If it is then check the Class of Restriction of the routes in the route list or plan. **Note:** Before you change Class of Restriction to enable chargeable calls make sure that you have the authorization of the customer. **Tip**: Use the SMDR records to assist you.
			Page 1 of 7

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
Any	Calls are being cut off	• Trunk programming error • Hardware issue • Wiring fault	Check for a pattern. • Are the calls always being made to the same number? • Is it a cellular phone? If it is it is likely to be a cellular issue. • Is this affecting many users or just one? Build a pattern. • Many Users - Check SMDR records to see if it is a particular trunk or link that is causing the problem. • One User - Ensure that it is not a hardware or wiring issue.
Any	An internal caller does not get a busy signal when calling a busy internal station.	A busy signal is not returned to the caller when the call is immediately camped onto another internal station that is in the busy stated. This can be caused by the Class of Service (COS) option Auto Camp-on Timer being set to 0 (zero).	In the Class of Service Options: • Disable the Auto Camp-on Timer option by blanking the option field. OR • Increase the Auto Camp-on Timer to a number larger than zero (e.g. 10 seconds).
Any	User reports that they are continually receiving incorrect calls.	System or set programming error	Establish if the calls are always for the same person or if they are for different people. If the calls are always for the same person check the following: • Telephone Directory to ensure that the name and extension number are correct. • The users number against that of the person people are looking for. If the numbers are similar then it is possible that people are dialing incorrectly. Changing the users extension number maybe an option. • That the person being called has not call forwarded or rerouted calls to the user (who raised the complaint) in error. If the calls are for different people try these options: • Ask the user to log the calls received in Error. • Check the SMDR logs to establish a pattern.
			Page 2 of 7

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
Any	Internal caller does not hear busy signal when calling an internal station in busy condition.(Busy signal is not returned to user when call is immediately camped on to another internal station that is in busy condition.)	COS option Camp On Timer is set to 0.	To correct • disable Auto Camp on by blanking Camp On Timer in COS, or • delay Auto Camp On by setting COS option- Camp On Timer to a value other than 0 (i.e. 10 seconds). By doing this, the call still Camps On, but only after the timer expires.
Any	The volume setting saved on the handset is lost.	The “Handset Volume Adjustment - Saved” parameter is set to “No”	Set the “Handset Volume Adjustment - Saved” parameter to “Yes” in the Class of Service Options form.
		The set is dual mode and the volume was set at its maximum. For hearing safety, dual mode sets are programmed to revert to their default volume setting if they are saved at maximum volume	On a dual mode set, save the volume at least one setting level below maximum to ensure that it will be saved.
Any	Phantom calls are being made to the operator.	When a user hangs up without completing an operation in his or her voice mail box, the embedded voice mail continues to perform its function with whatever portion of the user's input is available, even though the user has hung up, and performs off-hook dialing in attempt to complete the operation. Often, this results in calls to 0, usually the operator.	In the Class of Service Options form, set the Multiline Set On-Hook Dialing option to “No”.
Any	Unable to put DID call on hold.	If you have **Record-a-call Save Recording on Hangup** enabled, you won't be able to put DID calls on hold.	In the Class of Service Options form: • Disable **Record-a-call Save Recording on Hangup**.
			Page 3 of 7

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
ONS Sets	ONS sets not ringing on a peripheral node, AX controller, or ASU; however set can be answered and a two-way conversation carried out.	Frequency-Shift Keying (FSK) is not assigned in the PSC DSP (Peripheral Switch Controller/Digital Signal Processor) form, and the ONS sets have COS CLASS/CLIP option enabled.	1. Assign FSKs, or 2. Turn off ONS CLASS/CLIP in the ONS Class of Service.
	ONS sets not ringing on an AX controller, or ASU II.	Maximum number of ONS supported on an AX controller or ASU II has been exceeded.	Number of ONS sets supported by the AX controller or ASU II has been exceeded. Refer to the Engineering Guidelines for details.
Analog set	The analog set on an ONS port experiences a “No dial tone” problem when the message waiting lamp is ON.	The AX controller may be running 3300 Rel 7.1.3.4 or earlier.	• You can patch the software load on the AX controller(s). Download 3300_Patch_7.1.3.6.zip from Mitel OnLine. OR • You can install or upgrade the AX Controllers in your system with the most recent post-7.1 software load.
Single-line Analog sets	Message lamp fails to function.	Insufficient voltage. The ASU and ASU II bays only support message lamp activation at 90 volts. Some single-line telephones require 110 volt message light activation.	Some set models will support either 90 volts or 110 volts via dip switch settings, Contact your supplier to determine if the sets support message lamp activation at 90 volts.
Analog or DNI Phone	No Dial Tone	Multiple possible causes	See “No Dial Tone - Analog or DNI Phone” on page 191.
Display Phones	Display phone that receives an incoming call transferred from another station does not shown name or number for incoming calls. Instead, the final answer point displays the transferring party information.	Calls which into the system over ISDN using 4ESS protocol do not deliver name or number on the display.	Refer to Mitel Knowledge Base article 06-5104-00034.
IP Phone	No Dial Tone	Multiple possible causes	“No Dial Tone - IP Phone” on page 193
			Page 4 of 7

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
IP Phone	IP Phone fails to boot	Network Connection.	Verify network connection
		No power	Verify power (is there a display?)
		Faulty wiring or connection	Check the wiring and connections
			Check LED on the IP telephone for network activity. • A green LED on the bottom of the phone indicates a proper connection • A flashing red LED indicates activity (data flow) on the network.
IP Phone	IP Phone fails to boot.	Set's IP address cannot be reached.	Use the PING (Packet Internet Groper) on the IP telephone to determine whether the server's (3300 ICP, DHCP, and/or TFTP) IP address is accessible.
		DHCP programming.	Ensure that the DHCP server has been programmed with the correct information. If a DHCP server is on the 'other side' of a router from the IP phone, then the router must have DHCP forwarding enabled. **Note:** IP sets require a firmware upgrade to support the new DHCP options introduced in 3300 Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-135 must be present in the DHCP server. After the sets have booted, options 128-135 may be removed to avoid future conflicts with standardized or other vendors use of these options. If the IP telephone displays "TFTP LOAD FAILURE" verify that the TFTP Firmware, DSP and Main. software loads are available and not corrupted.
			Page 5 of 7

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
		Phone is not registered with the system.	Register phone with system. See Register IP Phones in the Programming book of the System Administration Tool online help. Also see Table 18, “IP Phone Registration Troubleshooting,” on page 70
IP Phone	IP Phone stuck at “lock-out” or “pin in memory”.	The PIN registration code and the extension number of the IP phone are saved in the flash memory of the phone. A potential issue evolves when IP phones are moved from one site to another. If the IP phone has been successfully registered with system A, moving this phone to system B will cause it to fail and it will be stuck at “lockout” or “PIN in memory”.	Ensure that the site is using IP clustering before following these steps to clear the memory. 1. Clear the PIN registration code and the extension from the flash memory of the IP phone, by pressing the * key for a few seconds while powering the IP phone. 2. After the flash memory is clear, the IP phone will prompt you to enter the PIN as usual in a new system.
	Network ICMP Redirect Packets may cause “Exception Errors” in IP Phones which may result in unexpected reset.	Network ICMP Redirect Packets causing “Exception Errors” in IP Phones resulting in unexpected reset.	Refer to Mitel Knowledge Base article 08-5157-00024.
	PC Port not functional	COS option “PC Port On IP Phone - Disable” is set to Yes.	In the Class of Service Options form, change “PC Port On IP Phone - Disable” option to No.
IP Phones	After Cisco firmware upgrade, phones do not respond to 802.1x/EAP request.	Cisco firmware 12.2.5SE2 supports 802.1x/EAP version 3, Mitel IP phones do not recognize version 3 requests and ignore them.	Upgrade phones that support 802.1x versions 1 and 2: • 53xx phones: Upgrade firmware to 4.0.0.26. • 52xx phones: Upgrade firmware to 2.5.0.5.
			Page 6 of 7

Table 15: General Phone Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
IP Phones (Dual Mode)	Dual Mode phone fails to boot up.	Dual mode phones may fail to boot up for two different reasons: 1. Cisco Discovery Protocol (CDP) is not supported in certain loads. 2. You cannot downgrade the Boot Loads in dual mode sets and they are not compatible with the Main Load in 5.0.5.5.	Refer to Mitel Knowledge Base article 04-5173-00019.
	Dual Mode phone does not retain the increased volume after user hangs up.	Dual mode sets reset to the default volume of level 4 if a user changes the volume to the maximum level of set and then hangs up.	Refer to Mitel Knowledge Base article 06-5173-00037.
SIP Phones	Phone fails to register. Responds with "404 not found" even though SIP extension username/password matches the MCD generic SIP extension/pin.	ARS Maximum Dialed Digits for COR 1 is set to a value less than the SIP phone DN length.	Set ARS Maximum Dialed Digits for COR 1 is set to a value equal to or greater than the SP phone DN length.
			Page 7 of 7

Issues with Specific Models

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
5560 IPT	Only the left handset is functioning. The right handset is not operational.	Directory number is not assigned to the 5560 IPT Slave.	In the 5560 IPT Master/Slave Association form, assign a Slave directory number.
			Page 1 of 7

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
5235, 5320, 5330, 5340, 5360 IP Phone	A 5235 IP set loses all application features (including People, Messages, History, Settings and Applications) and Labels after the set is rebooted. OR A 5235, 5320, 5330, 5340 or 5360 set loses all applications after the 3300 ICP IP address is changed.	The controller address does not match the ICP/PBX assignment.	1. Program Network IP address in the ICP/PBX Networking form to match IP address of the local controller. 2. Reboot the controller to make the change effective.
SUPERSET 4000, YA, and IP Phones	Headset issues.	Attempting to use an unsupported headset.	Refer to Mitel Knowledge Base article 05-6778-00015 for a listing of supported headsets.
5235 IP Phone	People, Messages, History, Settings, and Application shutters on the 5235 IP Phones do not function.	If you change the IP address of the RTC on the 3300 ICP (System IP address on MXe Server), the 5235 IP Phone applications will not function.	To restore these applications: 1. Program a local entry in the ICP/PBX Networking form that matches the new IP address of the RTC (or System IP address on MXe Server) or If you already have an entry in the ICP/PBX assignment (hot desk or clustered systems), change the local entry to match the new RTC IP address or System IP address. 2. After you program the local entry, reboot the 3300 ICP and the 5235 IP Phones will recover all the applications.
			Page 2 of 7

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
5702 IP Phone or SpectraLink Wireless Handset	User experiences audio interruption on either of these sets. User is in a conversation on either of these phones and a programmed key becomes active (for example, ringing or receiving calls) and the user experiences a momentary interruption in audio reception.	The 5207 IP Phone has 14 programmable keys; the SpectraLink wireless set has 13 line select keys. If you program Direct Station Select (DSS) or multiline key appearances with audible “ring” type into any of the programmable keys on these phones, users may experience audio interruption during calls.This interruption occurs because the hardware in these phones does not support two speech channels.	Do not program DSS or multiline key appearances with “audible” ring type on 5207 IP Phones or SpectraLink wireless sets. If you need DSS or multiline key appearances on a phone, you should program the key appearances on the 5207 IP Phone or SpectraLink wireless set with “no ring” type, or use an IP Console (Release 5.2 version or later), a 5215 IP Phone, or a 5220 IP Phone instead of the 5207 IP Phone or SpectraLink wireless set.
5140 or 5240 Webset Phones	The following error appears in the display: WEB BROWSER ERROR # 2 Domain Name Service (DNS) Timeout Host Name was not resolved.	DHCP Server setup.	To resolve this problem, you have two options: **Option A:** 1. In your DHCP server, program Mitel proprietary Option 135 (Proxy Server) as String type and enter a socket value in the format of <ip:port> For example: 192.168.1.4:3128 where 192.168.1.4 is the IP address of the MSL server and 3128 is the http proxy port 2. Reboot the webset to get the new DHCP option. **Option B:** 1. Program the MSL server to also be your DHCP server. For information on how to configure the MSL server, refer to the Mitel Standard Linux (MSL) Installation and Maintenance Guide available from Mitel Online 2. Reboot the webset to get the new DHCP option.
			Page 3 of 7

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
Norstar Phones	Fails to register. Remains in DHCP discovery.	The CITELlink gateway contains two Network Layer Processors (NLPs) referred to as NLPA and NLPB. Each processor supports 12 phones and the processors require their own unique IP addresses. When using DHCP, the DHCP server must have at least two spare IP addresses (one for each NLP).	Enter a unique IP address in the myIPAdress field of both the NLPA and the NLPB forms. In addition, we recommend that you connect the CITELlink gateway to the ACCESS PORT of the Layer2 switch for the associated VLAN. Refer to the *3300 ICP CITELlink Gateway Installation and Configuration Guide* for instructions.
5x40 IP Phones	5x40 IP Phone will not function.	If you attempted to use the 5x40 phone Visual Voice Mail feature before enabling the COS option “HCI/CTI/Tapi Monitor Allowed”, the phones will not function even after you enable the COS option.	Refer to Mitel Knowledge Base article 04-3849-00010.
5224 IP Phone	After reset of phone, phone display stuck at “Upgrade part 3 14% Do Not Power Down”.	If you reset a phone during its upgrade process, the phone's flash memory will become corrupted.	Refer to Mitel Knowledge Base article 06-4409-00020.
5220 with 5422 PKM	Any of the following: • one way audio when using speakerphone (microphone will not transmit) • Dual mode 5220 phones will not boot and will show “INIT ERROR PKM INFO INCOMPATIBLE” error • Dual mode 5220 phones will not boot and will show “NO INIT ERROR PKM CARD INCOMPATIBLE” error	Unsupported hardware revisions.	Refer to Mitel Knowledge Base article 04-3849-00863 for the minimum required hardware revisions.
5330, 5340, 5360 IP Phone	No audio streaming to the corded handset.. 5330/5340 running firmware 1.6.2.4 or higher. 5360 running firmware 3.0.2.10 or higher.	Set not set up for handset operation.	Do either of the following: 1. Unpair the Cordless Handset (see 5330/5340 User Guide for instuctions). or 2. Power down the Cordless Handset (silmulaneously hold Mute and Volume down on Cordless Handset)
			Page 4 of 7

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
A 5215 Dual Mode, 5220 Dual Mode, 5235, 5304, 5312 and 5324 IP	Phone fails to boot up. Set display shows “Port Access Control – Press # to Continue”.	802.1X port authentication is enabled in network, but IP phone is not configured with a username and password.	Configure username and password on IP phone. See *“Configuring an Authentication Username and Password” on page 199*. OR Disable 802.1X support in the Layer 2 switch. See *“Enabling or Disabling 802.1X Authentication” on page 201.*
A 5215 Dual Mode, 5220 Dual Mode, or 5235 IP	Phone fails to boot up. Set display shows “Port Access Failure – Rebooting”.	802.1X port authentication is enabled in network. IP phone is not configured with correct username and password.	Check the username and password of the IP phone in database of the RADIUS server. Configure the correct username and password in the IP phone. See *“Configuring an Authentication Username and Password” on page 199* OR Erase the username and password that is stored in the phone. See “Erasing an Authentication Username and Password” on page 200. Reboot the phone in order to re-enter the username and password.
		802.1X port authentication is enabled in network. PC is connected to network through IP Phone, but PC is not configured with correct username and password.	Check the username and password of the PC in database of the RADIUS server. Configure the correct username and password on the PC. OR Disable 802.1X support in the PC if enabled. OR Ensure RADIUS EAP is “EAP-MD5”.
5235, 5320, 5330, 5340, or 5360 IP sets	Phone loses all application features and labels after the set is rebooted or after the 3300 ICP IP address is changed.	The controller address does not match the ICP/PBX assignment. 1. Program Network IP address in the ICP/PBX Networking form to match IP address of the local controller. 2. Reboot the controller to make the change effective.	See Mitel Knowledge Base article 07-4940-00007.
			Page 5 of 7

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
53xx IP Sets	Phones stuck at DHCP discovery after upgrade to MCD 5.0 SP1.	Misconfiguration issue between Layer 2 switch port and DHCP server. Prior to MCD 5.0 SP1, the 53xx IP Phones would accept both untagged and tagged frames even though they send tagged frames with VLAN ID of N (where N is a value from 1 to 4096.) In MCD 5.0 SP1, the firmware for 53xx IP Phones changed to adhere to the industry-standard behavior for VLAN aware devices as follows: when the DHCP server offers option 125 with VLAN ID of N, the IP Phone releases its current IP address and sends VLAN N-tagged DHCP discovery. The DHCP server responds with a DHCP offer tagged with VLAN N. In a typical VLAN aware device, all outgoing/incoming frames are expected to be tagged.	Reconfigure network on the basis of the following rule of thumb: If VLAN ID and Priority are assigned to DHCP option 125, L2 port is expected to send and receive Tagged frame with VLAN ID (In Cisco term, L2 port is configured as a Trunk port). Examples and solutions to some of the network misconfiguration: ***Case 1*** ========== **L2 port setting (to which 53xx is connected):** Access port (untagged) for VLAN ID of N. **IP phone obtains VLAN ID via:** DHCP option 125 is configured with VLAN ID of N, and priority of N. **Solution:** • Remove the VLAN ID from DHCP option 125. or • Make the L2 port and access port tagged for VLAN N. ***Case 2*** ========== **L2 port setting (to which 53xx is connected):** Access port (untagged) for VLAN ID of N. **IP phone obtains VLAN ID via:** From the LAN policy of LLDP/CDP. **Solution:** Make the L2 port a trunk port tagged for VLAN N. ***Case 3*** ========== **L2 port setting (to which 53xx is connected):** Access port (untagged) for native VLAN. **IP phone obtains VLAN ID via:** DHCP option 125 is configured with native VLAN ID of 1 and priority. **Solution:** Remove VLAN 1 and priority from DHCP option 125.

Table 16: Specific Model Troubleshooting

Phone	Symptom	Probable Cause	Corrective Action
5310 Conference Unit	5310 Conference is not working with 5220 DPLite (Dual Mode IP phone). The symptoms are when a user pushes the side control button, the saucer flashes but does not work.	Side control defective.	Refer to Mitel Knowledge Base article 06-5191-00067.
			Page 7 of 7

IP Phone Power

Table 17: IP Phone Power Troubleshooting

Symptom	Probable Cause	Corrective Action
Power unit is plugged in, but does not power up.	No power at outlet. *OR* faulty power outlet. *OR* faulty power cord.	1. Plug a known functioning device in the power outlet. 2. Verify that the power outlet protection circuit has not tripped. 3. Verify that the voltage of the power outlet is within specifications. 4. Verify that the Power Unit power cord works correctly (including good and solid ground connection).
	Faulty power connections.	Verify the following: • Ensure power is applied to the power unit. • Ensure you are not using crossover Ethernet cables. • Ensure that the input Ethernet cable is connected to the **Data In** port of the power unit. • Ensure that the output Ethernet cable is connected to the **Data and Power Out** port of the power unit. • Ensure that the input and output cables of a port pair are used for the same IP Phone.
		Page 1 of 4

Table 17: IP Phone Power Troubleshooting

Symptom	Probable Cause	Corrective Action
IP device does not work, and both Port Status LEDs are OFF (Power unit is not detecting IP device).	Wiring problem OR faulty IP device OR faulty Power Unit.	1. Verify you are using a standard UTP Category 5, 6 or 6e cable (with 8 wires–4 pairs). 2. Verify that you are not using a crossover cable. 3. Verify that the connections for the port pair both correspond to the same IP device, and that the port connections are not reversed. 4. Verify that the cables connected to the Data In and Data Out ports correspond to the same IP device. 5. Connect the IP device to a different port pair on the Power Unit. If the device works normally, the original port is probably faulty. 6. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty. 7. If possible, connect the IP device to a different Power Unit. If the device works normally, the original Power Unit is probably faulty.
IP device that receives PoE from a CXi controller port is not powering up.	Maximum PoE has been exceeded. The CXi controller provides a maximum 100 Watts for PoE.	Refer to the Engineering Guidelines for information on how to engineer PoE for the system.
	Power over Ethernet has been disabled for the IP device port	In the System Administration Tool check the Layer 2 (L2) Switch form. Ensure that the Power over Ethernet is set to “Auto” for the port.
		Page 2 of 4

Table 17: IP Phone Power Troubleshooting

Symptom	Probable Cause	Corrective Action
IP device works, but there is no data link.	Wiring problem OR Faulty IP device *OR* Faulty Power Unit. *OR* Missing/faulty local power adapter.	1. Verify that the port's Power Active LED is continuously ON. 2. Verify that the connections for the port pair both correspond to the same IP device, and that the port connections are not reversed. 3. The IP device may require a local power adapter to operate. If an adapter is already in use, replace it with a known working adapter. If this works, replace the faulty adapter. 4. Verify you are using a standard UTP Category 5, 6 or 6e cable (with 8 wires–4 pairs). 5. Verify that the cable length between the Power Unit and the IP device does not exceed 100 metres. 6. Verify that you are not using any crossover cables. 7. Verify that the Power Unit is connected to a switch/hub with a good RJ-45 patch cord connection. 8. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty. 9. Try to connect a known working IP device to the same port (test device). If the test device works and the link is established, there is probably a faulty data link in the original IP device. 10. Connect the IP device to a different port pair. If the device works, one of the original ports is probably faulty, or there is a bad RJ-45 connection.
		Page 3 of 4

Table 17: IP Phone Power Troubleshooting

Symptom	Probable Cause	Corrective Action
IP device not operating, with Power Inactive LED ON.	Discharged capacitor in IP device OR wiring problem OR missing/Faulty local power adapter OR faulty port.	1. Wait 5 to 10 seconds. If the Power Active LED turns ON, there was a discharged capacitor in the IP device. 2. Verify that you are not using any crossover cables. 3. The IP device may require a local power adapter to operate. If an adapter is already in use, replace it with a known working adapter. If this works, replace the faulty adapter. 4. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty. 5. Connect the IP device to a different port pair. If the device works, one of the original ports is probably faulty, or there is a bad RJ-45 connection. 6. Unplug the IP device, and verify that the Power Inactive LED turns OFF. If it does not, the port is probably faulty, or the RJ-45 socket is shorted.
IP device powered correctly, but Power Active LED is OFF.		Re-connect the IP device to a different port pair. If the new port pair Active Power LED turns ON, there is a fault in the original output port (probably a faulty LED).
IP device does not work, but Green Port Status LED ON.	Wrong connection *OR* faulty IP device.	Verify that the IP device is actually connected to that port. Replace the device by a known working IP device (test device). If the test device powers up, the original IP device is probably faulty.
		Page 4 of 4

IP Phone Registration

1. Record the error message on the IP Phone display, then go through **Table 18**.

Tip: To rule out DHCP problems, and isolate network-related issues, we recommend that you program the IP Phone with a static IP Address.

Note: IP sets require a firmware upgrade to support the new DHCP options introduced in 3300 Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-133 must be present in the DHCP server. After the sets have booted, options 128-133 may be removed to avoid future conflicts with standardized or other vendors' use of these options.

2. If you still can't fix the problem collect the following information and then call Mitel Technical Support:

   ❒Is the problem with the local or remote subnet?

   ❒DHCP server(s) settings

   ❒Layer 2 switch configuration and settings

   ❒Router configuration and settings

   ❒Network Diagram

   ❒IP addressing scheme

   ❒VLAN configuration and settings

Tip: Use the debug option on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, and memory Stats details (see page 159).

Note: If a 3300 system is enabled with the MLPP feature, the IP phones that register to this controller are in an enhanced security mode. You will be unable to access the full phone debug menu because the IP phone is locked down from a security perspective. To bring the IP phone out of lock down mode, you must register the IP phone to a 3300 controller that does not have MLPP enabled. You must redirect the IP phone with DHCP options (that is, change DHCP Server option (option 125) so that IP phone will register to a 3300 controller that is not running MLPP mode). After the IP phone is successfully registered to a 3300 controller that is not in MLPP mode and after the phone has been up and running for approximately 20 seconds, you will be able to access the full debug menu.

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
Invalid VLAN ID	DHCP Option 43 or 125 on 3300 Release 7.0 or later systems or 132 and/or 133 for earlier releases not set correctly.	1. Identify the location of DHCP server and which DHCP server is assigned the IP address for the corresponding subnet (see "Network Configuration Examples" in the "Typical Network Configurations" chapter of the *MCD Technician's Handbook* for examples). 2. For an external Microsoft DHCP server (NT server, etc.), make sure that the option type is set to LONG. 3. For a Cisco® Router DHCP server, make sure that the option type is set to hex, and padded with 0s (for example, 0x00000002 for VLAN 2). 4. For the controller internal DHCP server, set the option type to numeric.
Duplicated IP address	Existing data device owns the IP address.	1. Check the IP address on the phone display. 2. Disconnect the IP Phone. 3. From a PC on the same subnet, ping the suspected IP Phone. If there is a response, identify the data device, and resolve the conflict.
	Corrupted DHCP server.	1. On the suspected DHCP server, disable then recreate the scope. 2. If this is a Microsoft DHCP server, reboot the server.
		Page 1 of 7

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
DHCP discovery *OR* DHCP OFFER X REJ	DHCP option 43 or 125 on 3300 Release 7.0 or later systems or option 130 (MITEL IP PHONE) for earlier Releases is not programmed.	Identify the location of DHCP server and set to Option 130 as String type with value of “MITEL IP PHONE”.
	DHCP server does not have enough IP addresses.	Create a larger scope with more IP addresses on the DHCP server.
	DHCP server cannot assign IP addresses for the corresponding subnet, even though there are enough IP addresses.	1. For a Microsoft DHCP server, reboot the server. 2. For the controller internal DHCP server, disable DHCP and rebuild the scope.
	L2 switch port is shut down or not configured properly.	1. Check the L2 switch, and ensure that the port is not shut down. 2. Ensure that this port can access the DHCP server subnet (that is, access the port for the same VLAN, etc.).
	Your installation is using the controller’s internal DHCP server, but DBMS Save is not on.	Enter the DBMS Save command through the Maintenance Commands form.
		Page 2 of 7

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
DHCP Discovery OR DHCP OFFER X REJ (VLAN) (after releasing the first IP from the native DHCP server)	DHCP Option 43 or 125 on 3300 Release 7.0 or later systems or Option 30 (MITEL IP PHONE) for earlier Releases is not programmed on the second scope of the DHCP server (or on the second DHCP server). OR VLAN ID is not assigned properly.	1. Identify if there is one DHCP server for both VLANs, or if there is one DHCP server per VLAN (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the *MCD Technician’s Handbook*). 2. For one DHCP server for both VLANs, ensure that option 43 or 125 is properly configured (3300 Release 7.0 and later) or that option 130 is programmed as String type with value of “MITEL IP PHONE“ (prior to Release 7.0), in the scope of Voice LAN. 3. For one DHCP server per VLAN, ensure that option 43 or 125 (Release 7.0 and later) or 130 (prior to Release 7.0) is defined. 4. Verify that the proper VLAN ID is assigned in option 43 or 125 (Release 7.0 and later), or 132 (prior to Release 7.0).
	One DHCP server for two VLANs network configuration: IP helper address on the router interface is not set up correctly.	1. On the router interface (on which DHCP is not residing), enter the IP helper address and specify the IP address of the DHCP server on the other side of the subnet (that is, always set up IP helper address on the DHCP server client side). 2. Ensure the second scope is created for the corresponding VLAN (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the *MCD Technician’s Handbook*).
		Page 3 of 7

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
(Cont'd)	The L2 switch port for the phone interface is shut down or not configured properly.	1. Check the L2 switch and ensure that the port is not shut down. 2. For a Cisco L2 switch, ensure that this is a trunk port with Dot1q encapsulation, and that this trunk port allows both native and Voice LAN to pass through. 3. For an HP L2 switch, ensure that Native Lan is untagged, and that Voice LAN is tagged. 4. Verify whether there are two physical interfaces to the router (one per VLAN), or a router on a stick configuration (one physical with virtual sub-interfaces). 5. Ensure that the ports on both sides (L2 switch and router) are not shut down (See "Network Configuration Examples" in the "Typical Network Configurations" chapter of the *MCD Technician's Handbook*). 6. If there is a physical interface on the router for each VLAN, make sure that the L2 switch is set to correctly access port for the corresponding VLAN/ subnet. 7. If there is one physical interface on the router for multiple VLANs, ensure that this is a trunk port on the L2 switch, and ensure that this trunk port allows both native and voice LAN to pass through. 8. On the router sub-interface, ensure that the proper VLAN is associated to the remote sub-interface.
		Page 4 of 7

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
TFTP load failure	DHCP option 43 or 125 on 3300 Release 7.0 or later systems or option 128 for earlier releases is not set up to point to the right TFTP server (Controller).	Check the DHCP server, and confirm that option 43, 125, or 128 is pointing to the right TFTP server.
	No network connectivity between the controller and the phone.	1. Confirm that the controller is connected to the network. 2. For a Cisco L2 switch: verify that the L2 switch is access port (Voice LAN). 3. For an HP L2 switch: verify that the L2 switch is untagged (Voice LAN). 4. If the router is involved, make sure that the router's MTU is set to 600 or more.
	Firmware on controller is missing or corrupted.	1. Verify that the firmware (**ipp510bootenc.bin**, etc.) is in the **sysro/tftp** directory (particularly if the user has manually copied the firmware). 2. Confirm if TFTP on the controller is corrupted (this can be verified by connecting the IP Phone directly on the controller, or by observing the behavior of other IP Phones). **Tip:** If you have Option 132/133 programmed on the controller's internal DHCP server, disable them before trying Step 2.
	Your installation is using the controller's internal DHCP server, but DBMS Save is not on.	Enter the DBMS Save command through the Maintenance Commands form.
Waiting for link	DHCP option 43 or 125 on 3300 Release 7.0 or later systems or option 129 for earlier Releases is not programmed correctly.	Check Option 43, 125, or 129 on DHCP to confirm that the IP address is programmed correctly. (RTC IP Address of controller; for the MXe Server, use the controller System IP address.)
	Spanning Tree protocol is disabled. It's used to provide location and location information for Emergency Services (E911).	Ensure Spanning Tree protocol is enabled.
	The application server is broadcasting or multicasting on IP Phone port or on PC behind the IP Phone.	Turn off multicasting.
	The PC behind the IP Phone is changing speed 100/10.	Depending on the NIC, you may need to hardcode to 100 MBps instead of auto negotiation.
		Page 5 of 7

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
Waiting for link *OR* Lost link to Server	IP phone fails to receive Keepalive message in 30 seconds.	Verify if the network or the controller is down.
	There is electrical interference.	Verify the power source, and change the location of the power source.
Unable to register IP phones due to regproc trap. Other symptoms once a regproc trap has occurred are as follows: • Can't reregister a phone that was already registered. • Can't log in hot desk users. • Phone stays up after deleting a MAC.	IP Phone has tried to register more than 10 times in succession without success.	Refer to Mitel Knowledge Base article 06-9999-00024.
		Page 6 of 7

Table 18: IP Phone Registration Troubleshooting

Error Message on Display	Possible Cause	Corrective Action
TFTP Fail (Remote IP phone (statically programmed IP address) cannot access MN3300 across WAN).	The Layer 2 switch port for the phone interface is shut down or not configured properly.	1. Check the Layer 2 switch and ensure that the port is not shut down (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the *MCD Technician’s Handbook* for more information). 2. For a Cisco Layer 2 switch: verify that this is a trunk port with Dot1q encapsulation, and ensure this trunk port allows both native and voice LAN to pass through. 3. For an HP Layer 2 switch: verify that Native Lan is untagged and Voice Lan is tagged.
	The Layer 2 switch port for router interface is shut down or not configured properly.	1. Verify which configuration you have (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the *MCD Technician’s Handbook* for more information). 2. Ensure the port(s) on both sides (Layer 2 switch and router) are not shut down. 3. If there is physical interface on the router for each VLAN, make sure that the Layer 2 switch is set to access the port for the corresponding VLAN/subnet correctly; *OR* If this is a router on a switch, verify that this is a trunk port on L2 switch, and ensure this trunk port allows both native and voice LAN to pass through. 4. On the router's sub-interface, verify that the proper VLAN is associated to the sub-interface (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the *MCD Technician’s Handbook* for more information)).
(Cont’d)	Typo in IP address, VLAN ID, gateway.	1. Delete and reprogram the static IP address. If there is no VLAN or priority, leave them as blank. 2. Verify that the gateway IP address is correct.
		Page 7 of 7

Phone Connection

Tip: On display IP phones use the Configuration (Debug) Menu to view Version, Network, Telephony/DSP, Connection Browser Config, memory Stats details (see page 193).

Table 19: Troubleshooting Phone Connection Problems

Symptom	Possible Cause	Corrective Action
Cannot make outgoing calls (except for emergency and attendant calls). “License Violation” displays on idle DNI and IP sets.	The controller is in System Lock license violation mode.	Correct the license violation event by reducing the number of over-allocated licenses.
Cannot make calls externally (display phone may show **call barred**).	COR restricted.	1. Identify the numbers dialed by the user, then check the route used in ARS. 2. Remove the COR number from COR group table in COR assignment used in the route, *OR* Change the COR group number in the ARS Routes form.
	COS restricted for PRI or QSIG trunk.	Enable **Public network access via DPNSS** in the set's COS.
Cannot make call over analog loop trunk (intermittent problem).	PBX is sending the dialing digits too fast for Telco's receiver on the LOOP trunk.	Insert a tone plan in the ARS Digit Modification Plans for the route used by analog loop trunk (tone plan is used to insert one or two seconds delay without any tone detection).
NONE of the sets are responding.	Problem with controller.	Perform a system check on the controller.
Sets cannot receive DID calls.	Non-DID is enabled in Station Attributes form.	Disable non-DID in the set's COS.
No dial tone on set.	Set is not programmed.	In System Administration Tool, program the extension accordingly.
	Wrong wiring.	Check the wiring between the phone jack and the ASU, peripheral cabinet, MDF, etc.
	Faulty handset wire.	1. Replace the handset cord. 2. Replace the handset. 3. Replace the set.
	Circuit is busy.	1. Enter the Maintenance command STATE <plid of the circuit>. 2. Enter the Maintenance command RTS <plid>.
	Circuit is locked out.	Verify the wiring between the phone and the patch panel.

Page 1 of 2

Table 19: Troubleshooting Phone Connection Problems

Symptom	Possible Cause	Corrective Action
No dial tone on set when message waiting lamp is on.	AX controller is running pre- 3300 7.1.3.6 software.	Patch with the 7.1.3.6 load (3300_Patch_7.1.3.6.zip from Mitel OnLine, OR Update the AX controller with the most recent post-7.1 software load.
Sets take 10-12 seconds to receive incoming calls.	ANI/DNIS number delivery trunk option is enabled in T1 trunk's COS.	Disable the ANI/DNIS number delivery in the trunk's COS. **Tip:** You can assign an unused COS to verify if this is the problem.
	Dialing digit conflict.	Check the following forms for any potential dialing conflict: - Station Service Assignment - Miscellaneous Assignment - Feature Access Code - Agent ID Assignment - System Option Assignment
IP to IP calls OK, but not IP to TDM calls (rings once, then call drops).	E2T not loaded.	1. Verify that the E2T IP address is programmed correctly. 2. Verify that the E2T IP address is not used elsewhere on the network. 3. If the E2T IP address was hard coded with a debug table, verify its settings (see "DHCP Configuration Settings" in the "Installation Planner:" chapter of the *MCD Technician's Handbook*).
Note: For IP Phone connection issues related to Resiliency, see "IP Device Resiliency" on page 159.		
		Page 2 of 2

Phone Audio Quality

Tip: Use the Configuration (Debug) Menu on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, memory Stats details (see page 194).

Table 20: Audio Quality Troubleshooting

Symptom	Prossible Cause	Corrective Action
One-way audio between Remote IP to TDM (VM)	No gateway IP address programmed on E2T.	1. If E2T gets IP address from DHCP server, make sure that Option 03 (Router) is assigned to the scope with the proper IP address for the subnet. 2. If E2T is hard coded with a static IP address, make sure that the gateway IP address is programmed properly in VxWorks.
		Page 1 of 4

Table 20: Audio Quality Troubleshooting(continued)

Symptom	Possible Cause	Corrective Action
Distorted audio only on NSU	Voice encoding is not inverted.	For T1, enable **invert** for Voice encoding in link descriptor. For CEPT or API, enable **ADI invert** for voice encoding. (This does not apply to Embedded PRI.)
Broken Audio, intermittent	Handsfree on the far end.	Ensure that neither device is using handsfree. Some handsfree phones only operate at half duplex.
	Packet loss, jitter via network.	1. Identify the speech path between the two end points, including router, switch WAN in the audio stream. 2. The network administrator needs to apply QOS/TOS to minimize jitter over slow speed interface (T1, Frame Relay, etc.), and give voice traffic priority over data.
	Limited bandwidth and too many calls across router, or combination data and voice.	1. Limit the number of calls to remote subnets. 2. The network administrator needs to apply QOS/TOS to give voice traffic priority over data.
	Physical port error (CRC, faulty cable, duplex mismatch, HUB).	1. Identify the speech path between the two end points, including router, switch WAN in the audio stream. 2. Verify that there is no duplex mismatch in each port settings, or faulty cable, or faulty port. 3. Make sure that the IP Phone is not plugged into a HUB.
	Compression zone enabled.	Compression will save bandwidth, but may cause noticeable clipping. If not sure, disable compression to see if it makes a difference.
	Router's CPU is exhausted or congested.	Router may be running excessive filtering. The network administrator may need to monitor the performance of the router.
Broken Audio, intermittent	Layer 2 Switch ports configured incorrectly.	1. In the Layer 2 Switch form of the System Administration Tool, configure all L2 ports in the voice path with the same settings. The recommended settings for the “Duplex Mode” field and the “Flow Control” field is “Auto”. 2. If the network requires fixed settings, use the following: - State - Enabled - Speed - 100 Mb - Duplex Mode - Full DX - Flow Control - Enabled - Voice VLAN - Tagged 3. If you change these fields to fixed settings, you must also set the IP phones to use the fixed settings. You change the IP phone settings through the Configuration menu. See “Access Configuration Menu on Single-Mode IP Phones” on page 194. 4. In the Configuration menu, select **Hardware Config?** and then select **Modify Port Setting** and modify the settings.

Table 20: Audio Quality Troubleshooting(continued)

Symptom	Possible Cause	Corrective Action
Echo occurring between IP Phones and TDM Phones	Handsfree mode is used.	Check if far end is using handsfree. Switch to handset mode to see if this corrects it, or lower the volume in handsfree mode.
	If echo occurs on calls between IP and TDM phones, the Echo Canceller could be beyond required specifications.	1. Identify the path between the two end points, and verify if Trunk is always involved. 2. Check with Telco to see if the trunk is within specs. On a typical T1, the input signal should be -15 dB. If it is too high(-5 dB for example), echo may result. If this is the case, keep an echo log to isolate the problem.
	Network jitter issue.	If the problem only occurs between IP devices, check network jitter issue above.
	Loop Start (LS) Trunk settings	If the problem occurs on phones that are connected via Loop Start (LS) trunks, use the Line Quality Measurement form in the System Administration Tool to test the line quality and to obtain the recommended settings.
		Page 3 of 4

Table 20: Audio Quality Troubleshooting(continued)

Symptom	Possible Cause	Corrective Action
Echo occurring between IP Phones	Layer 2 switch setting problem.	1. Check the L2 switch for duplex mismatch and spanning tree. 2. Turn off spanning tree between the L2 switch and the IP Phone if possible (use the PortFast setting). 3. In the Layer 2 Switch form of the System Administration Tool, configure all L2 ports in the voice path with the same settings. The recommended settings for the “Duplex Mode” field and the “Flow Control” field is “Auto”. 4. If the network requires fixed settings, use the following: - State - Enabled - Speed - 100 Mb - Duplex Mode - Full DX - Flow Control - Enabled - Voice VLAN - Tagged 5. If you change these fields to fixed settings, you must also set the IP phones to use the fixed settings. You change the IP phone settings through the Configuration menu. See page 194. 6. In the Configuration menu, select **Hardware Config?** and then select **Modify Port Setting** and modify the settings.
	Far end phone is on handsfree	Check if far end is using handsfree. Switch to handset mode to see if this corrects it, or lower the volume in handsfree mode. For best results when using handsfree mode: • ensure that the microphone (on the front edge of the telephone) is unobstructed and not close to a reflecting surface, such as a shelf. • minimize background noise (such as printers, fans, and radios) • sit within reach of the telephone • speak at a normal volume towards the microphone.
	In conference call, echo is noticed from external trunk	1. Identify the path between the two end points, and verify if Trunk is always involved. 2. Check with Telco to see if the trunk is within specs. On a typical T1, the input signal should be -15 dB. If it is too high(-5 dB for example), echo may result. Keep a log to isolate the problem.
	There is an audio path between the users as well as between the phones.	Provide better acoustic shielding between users, e.g. close the door, provide sound-deadening partitions.
Voice quality issues appear after a network upgrade	Cisco IOS is upgraded to IOS 12.2(37), Mitel IP phones receive DiffServ (DSCP) value of 0 from LLDP resulting in Voice Quality of Service degradation.	Refer to Mitel Knowledge Base article 08-5191-00104.
Audio issues on SIP, including Music on Hold	Need to have ENABLE_TX_CHAN_CONN feature enabled.	Refer to Mitel Knowledge Base article 11-5160-00010. **Note**: This feature is available only on MCD 4.x and above.
		Page 4 of 4

5550 IP Console

Table 21: 5550 IP Console Problems Troubleshooting

Symptoms	Probable cause	Corrective Action
5550 IP console fails to register (red LED is lit on TKB).	TKB (keyboard) - does not have a reserved IP address OR does not have the right IP address OR is not communicating with the right controller.	1. Check DHCP lease to confirm if an expected IP address is assigned to TKB. 2. If not assigned properly, ensure that you enter the MAC address of TKB properly in the Multiline Sets form in System Administration Tool. 3. Recycle the power of the TKB to ensure that the TKB is reloaded properly.
	Console PC does not have the proper IP address.	If the IP address of PC is on different subnet than the TKB, make sure that the router between these two subnets is functional.
	PC NIC has 802.1Q enabled on Data side while L2 switch is not configured to accept tagged frame on Native VLAN.	Disable 802.1Q on PC NIC **Note:** Only use 802.1Q on PC if PC and TKB are on the same VLAN (e.g 2) which L2 switch accepts tagged frame on the specified VLAN.
5550 IP Console fails to launch.	5550 IP Console has been registered and IP console is reinstalled.	Delete the MAC address from IP Consoles form and then re-register using the IP Console Configuration Wizard (Start/MN5550 IP console/Tools). **Note:** Do not reinstall the IP Console software unless you need to (new installation, corrupted software, etc.). You should always use the Configuration Wizard to register to a different controller.
	User does not have local administration privileges.	Add local administration privileges for the user.
"Unable to Display Page" Error Message when you launch Internet Explorer.	5550 IP Console is running on Windows 98 operating system on the PC.	Close the 5550 IP Console application and then open Internet Explorer. The 5550 IP Console must be run as a standalone application on Windows 98 (that is, with no other application open while it is running).
5550 IP Console Keypad not operating properly.	Required TCP ports blocked or conflicting with other applications.	Keypad to Console PC: TCP Port 6900, PC Port 10000 Console PC to 3300 ICP: Ports 6800, 7011, and 1606
		Page 1 of 2

Table 21: 5550 IP Console Problems Troubleshooting(continued)

Symptoms	Probable cause	Corrective Action
5550 IP Console stops working due to a pop-up error message that indicates that the console could not be started due to missing configuration settings.	In a resilient configuration the primary controller has failed over to the secondary, but the IP Console has not be configured as resilient (that is, it is not configured on the secondary controller).	You must configure the 5550 IP Console on the secondary controller. • For clusters that do not support Remote Directory Number Synchronization, you must manually configure the IP Console on the secondary controller. Refer to the *MCD Resiliency Guidelines* for instructions. • For clusters that support Remote Directory Number Synchronization, configure the IP Console with the secondary controller in the IP Consoles form.
		Page 2 of 2

CHAPTER 4

SOFTWARE

Software Troubleshooting Tips

- ☑ Always make a database backup before and after major database changes
- ☑ For troubleshooting issues that arise when you are using the MCD Software Installer Tool, see page 138
- ☑ For licensing issues, see “Licensing” on page 29.

System Software

Note: In the event of a system failure, collect the system error logs before contacting Product Support. Refer to Mitel Knowledge Base article 04-1000-00011 for instructions.

Table 22: System Software Troubleshooting

Symptom	Possible Cause	Corrective Action
Unable to download Mitel product software from Mitel Online	Microsoft Internet Explorer FTP option “Use passive FTP for compatibility ...." not enabled.	Refer to Mitel Knowledge Base article 04-1000-00022
	Corporate firewall configured to prevent access.	Configure corporate firewall to allow you to access and download product software from Mitel Online.
Loss of system database. After a scheduled reboot of the system, the 3300 ICP system database is blanked out.	If you decrease the IP user or IP device licenses in the License and Option Selection form, the system database is blanked out after the next scheduled reboot.	Perform a Database Restore from a recent system backup. If you reduce the number of IP user licenses or IP device licenses from the License and Option Selection form, always perform a DBMS Save prior to rebooting to prevent the loss of the database
System is not processing calls and appears to be locked up. **Note:** This procedure applies to controllers running 3300 Release 5.1.5.8 or later software.	Software issue	1. Run System Diagnostics: **For non-CX/CXi controllers only** • Locate the remote alarm On/Off button next to the Reset button on the front of the 3300 ICP controller. • Press and hold the remote alarm button until all alarm LEDs (critical/major/minor) are ON. • After you release the remote alarm button is released, the system reboots automatically within a short time. **For CX/CXi controllers** • Run the exeSysDbgCmds command from the RTC shell. 2. Collect logs for analysis after the system boot-up (see “To download the system diagnostics file to your computer” in the “System Diagnostics Reporting” topic of the online help). 3. Send logs to Mitel Technical Support for analysis

Software Installation and Upgrade

Table 23: FTP Server Errors

Error message on RTC shells	Possible Cause	Corrective Action
Fail to load file	IIS/PWS/FTP server is not running or not installed.	Go to your FTP site properties and re-start FTP services OR Re-install your FTP server.
	The installation files are not in the home directories of the FTP server.	1. Check and identify the home directory of your FTP site properties (default is c:/inetpub/ftproot), and ensure that **boot_install**, **sysro.tar** is there. 2. If the files are not there, run the **setup.exe** again to ensure that all these files are copied to this home directory (not the 3300 directory).
Fail to log in	FTP user (3300) cannot log in FTP server (by default, the FTP user defined in Vxworks is **ftp** and the password is **ftp**).	1. Check the security tab of your FTP site and ensure that your FTP site allows “anonymous” connection. 2. Verify if there is an FTP username defined in your FTP server's user domain. If there is, ensure that the username and password are correct, OR delete the user from user domain in order to allow “anonymous” login. 3. Confirm that the FTP user name and password in Vxworks are **ftp** and **ftp**. You may change them to match those defined on your server's user domain (or vice versa). **Tip:** You may ftp from a computer into the FTP server and login as user defined in Vxworks to confirm ftp user can access FTP server
	No network connectivity between your FTP server and the 3300 controller fails to log in	1. Ensure that your FTP server and the controller are on the same subnet. 2. If not, verify if the gateway IP addresses are defined, and that the router is able to route between two subnets. 3. If you changed the IP address on the FTP server, ensure that in “FTP site properties” you select the corresponding IP address on the FTP site tab. Typically, “unassigned”. 4. Verify that the Host IP address in Vxworks is pointing to your FTP server, and **bootdevice** is set to **motfcc**. **Tips:** To avoid troubleshooting router related issue, you should connect your FTP server directly to the controller (FTP server and controller on the same subnet).
	The Windows firewall and VPN firewall applications are enabled on the FTP server.	Disable the Windows firewall application and the VPN firewall.

Table 24: Upgrade Errors

Symptom	Possible Cause	Corrective Action
You install a 4 GB voice mail flash card into an AX controller that was previously up and running without voice mail installed. After you install the system software voice mail port 1 answers, but all other ports show “Out of Service”.	Proper voice mail partitions not set up on the new flash card.	Install the 4 GB voice mail flash card in the Flash 1 position. Reinstall the system software to set up the proper voice mail partitions on the card. **Note**: During the upgrade the Flash voice mailbox messages are lost. The AX Controller does not back up the voice mailbox messages prior to the upgrade. However, mailboxes, greetings, names and prompts are backed up

Backups and Restores

Table 25: Backup and Restore Troubleshooting

Symptom	Possible Cause	Corrective Action
Backup/restore failure (only fail to FTP files between PC). **Note:** If Java Plug-in console view is enabled, you should see the security warning.	Java version is not correct OR Higher version of Java is installed.	1. Verify that the correct version of Java is installed (Mitel supports Java 1.6.0_1 or later). 2. If another version is installed, remove it, re-install the correct version, and reboot the PC.
	Incompatible web browser installed.	1. Verify that the correct version of Internet Explorer or Mozilla Firefox is installed (Mitel supports IE 7.0 and later and Firefox 17 and later.). 2. If another version is installed, remove it, re-install the correct version, and reboot the PC.
	Backup/restore applet is not trusted (identitydb.obj not on PC).	1. Go to the Backup or Restore forms in System Administration Tool (Maintenance and Diagnostics). 2. Click the link to download the **identitydb.obj** file to the Maintenance PC. Save the file in: For Windows NT: WINNT/Profile/ <username>. For Windows 2000: Documents and Settings/<username>
	Backup/restore applet is not trusted (identitydb.obj not in right directory.	Verify the file is in the correct <username> profile (the profile used to log onto the PC).
	Backup/restore applet is not trusted (identitydb.obj has wrong extension).	Verify that the extension of the file is **.obj** (not .obj.obj, or .obj.txt, or anything else). **Tip:** Disable the Hide file extensions for known file types option to see the complete extension of the file. In the folder window, select: For Windows NT: View/Options/View. For Windows 2000: Tools/Folder Options/View.
Backup procedure repeats on its own	Internet Explorer timeout	Execute timeout.reg or timeout_4.reg from software CD/ Product_Support/Registry. (See README_for_timeout_reg_files.doc in Product_Support/Registry)
		Page 1 of 3

Table 25: Backup and Restore Troubleshooting

Symptom	Possible Cause	Corrective Action
FTP server responds with "permission denied" when attempting to write the backup file to the target directory.	FTP account missing DELETE permission on target directory.	Assign DELETE (in addition to WRITE) persmission to FTP account, then retry backup. See KB article 11-5191-00244 for additional information.
Database backup, with voice mail messages included, fails	Lack of free space in the db partition	Determine the amount of free space in the db partition and if there is enough space for voice mail messages. You can see the free space and required space by entering commands in the RTC window: • dosFsShow “/vmail” • debugVolInfo = 1 • debugVolInfo = 0 Refer to Knowledge Base Article 04-2806-00011 for detailed instructions.
Database backup fails on an AX controller	Voice Mail Flash is full	Delete Voice mails until there is enough space for the backup
Voice Mail messages are not backed up on an AX controller.	Voice Mail backup is not available on the AX	None
During a system database backup or restore you receive the following error message: “RAD group must be a number that will be DATA RESTORED before the pilot number”.	The leading digit of the hunt group number is lower than its RAD group number, so the system is unable to back up or restore the RAD group.	Program the leading digits of the hunt group pilot number to be greater than its RAD group numbers. When the system backs up or restores Hunt Groups, it does so in the order of the leading digits of the hunt group pilot number. See Hunt Groups in the System Features book of the System Administration Tool online help.
Unable to restore database	Attempting to restore a database from an AX Controller or MXe Server to a different type of controller.	You must restore an AX Controller database to an AX Controller. You must restore an MXe Server database to an MXe Server.
		Page 2 of 3

Table 25: Backup and Restore Troubleshooting

Symptom	Possible Cause	Corrective Action
Unable to browse to the backup file from the Restore dialog box	Your computer has does not have the required Java Plug-in version.	Install Java Plug-in version 1.6.0_01 or later. To browse for the backup file and to perform a backup, your current user account on the computer must have Java Plug-in version 1.6.0_01 or later installed.
Unable to perform a Data Restore from the Data Restore dialog box		Install Java Plug-in version 1.6.0_01 or later.
Unable to rename a new folder that you just created within the Backup dialog box or Restore dialog box.		Install Java Plug-in version 1.6.0_03 or later.
You receive the following message when you attempt to restore a database: “RAD group must be a number that will be DATA RESTORED before the pilot number.”	The leading digits of the hunt group pilot number are a lower number than its RAD group numbers. When the system backs up or restores Hunt Groups, it does so in the order of the leading digits of the hunt group pilot number. If the leading digit of the hunt group number is lower than its RAD group number, the system will be unable to back up or restore the RAD group data	In the Hunt Groups form, program the leading digits of the hunt group pilot number to be greater than its RAD group numbers.
You perform a database restore and ACD 2000 agent skill groups are missing from the database after the restore.	If the Extended Agent Group option is enabled and you have more than 128 agent skill groups programmed, when you perform a database backup, only the first 128 groups are saved.	Only the first 128 agent groups were saved to the database backup. Manually reprogram the missing agent groups
You are attempting to restore a pre- 3300 Release 6.0 database and receive the following error log: `Embedded System Music On Hold Audio source file size exceeds allocated space. It has been disabled and placed in a temporary location: db/temp/system_music_on_hold_tmp.`	If you restore a pre- 3300 Release 6.0 database, with an embedded music on hold file larger than 8 MB (for the MX/LX) or 16 MB (for the LX 512 MB), the file is moved to a temp location and disabled. The relocated file is not backed up and will remain on the hard drive until a full install is performed or until the file is deleted.	To restore music on hold when it is disabled due to file size: 1. Retrieve the **system_music_on_hold_tmp** file from **db/temp/** 2. Reduce the file size. Use the **System Audio Files Update** form in the System Administration Tool to restore the smaller music on hold audio file **OR** create a new audio file within the size limit.
		Page 3 of 3

If you still can’t fix the problem, call Technical Support. Make sure you have the following information on hand before calling:

- ❒ Java plug-in version

- ❒ Maintenance PC username
- ❒ Maintenance PC IP address
- ❒ Location of identitydb.obj file on the Maintenance PC
- ❒ Logs from the Maintenance Port (RTC Shell)
- ❒ MXe Server: Linux logs from /var/logs directory (via MSL web interface)

CHAPTER 5

SYSTEM FEATURES

System Feature Troubleshooting Tips

If you have programmed a system feature and the feature is not functioning as expected, ensure that:

- ☑ the feature is supported for the type of phone. Check the Phone-Feature matrix in the System Administration Tool online help to determine if a feature is supported on a specific phone type.
- ☑ you have programmed the feature correctly and reviewed the conditions that apply to the feature. Feature descriptions, conditions, and programming information are provided in the System Features book of the System Administration Tool online help
- ☑ the feature is enabled in the Class of Service (COS) that has been assigned to the phone.
- ☑ the Class of Restriction (COR) assigned to the phone is not preventing the feature from operating.
- ☑ System timers are set accordingly to allow system to activate feature (for example, Camp-on)
- ☑ the feature access code is programmed in the Feature Access Codes form and you have entered the Feature Access Code correctly, if the feature is activated via a feature access code
- ☑ another feature previously enabled on the phone isn't preventing the current feature from functioning. For example, Do Not Disturb could would prevent a phone from receiving a call.
- ☑ you have enabled the feature on the correct system, if you have multiple systems inter-connected in a network

The tables in the following sections provide specific feature troubleshooting information.

Features A to B

Table 26: Troubleshooting Features A to B

Feature	Symptom	Possible Cause	Corrective Action
Add Held	Unable to add a help call.	Record-a-Call is enabled on the phone. The Record-A-Call prompt takes precedence over the Add Held prompt.	Disable Record-a-Call feature in the Class of Service Options form.
	Unable to add a held call to a conference call on hold.	Functionality not supported.	None. Not supported on system.
Alpha Tagging	Alpha tagging not present on display phone for incoming calls.	Not supported for trunk type.	Only PSTN calls on the following trunk types support alpha tagging: LS Class, T1/D4, T1 CAS, T1 PRI, T1 QSIG, E1 PRI, E1 R2, E1 QSIG, and E1 BRI.
		Alpha Tagging entries not programmed in Telephone Directory form	Program alpha tagging entry for external telephone number
		Alpha Tagging not enabled in System Options form.	Enable option.
		Incoming signaling indicates that the caller's identity is private.	None. Not supported.
Advice of Charge	Not functioning.	Attempting to implement on non-European site.	None. Not supported in North America. Only supported with the Euro-ISDN (Euro-Standard variant) and Euro-BRI protocols.
		Carrier that provides the ISDN services is not delivering meter pulses for all applicable ISDN links.	Contact carrier.
		The specific variant of Advice of Charge is not supported by the system.	Refer to Advice of Charge in the System Administration Tool online help for a list of the supported variants.

Page 1 of 2

Table 26: Troubleshooting Features A to B

Feature	Symptom	Possible Cause	Corrective Action
Auto Answer	No audio over speakerphone.	Phone is not equipped with a speaker (for example, 5302 IP Phone).	Install a model of phone that has a speaker.
		Not supported for set type (for example, 5560 IPT and SpectraLink Wireless handsets do not support Auto Answer).	Refer to Phone-Feature Matrix in System Administration Tool online help.
		Call received from an incoming trunk where the set is programmed as the trunk's first answer point (e.g., DID or DIL).	None. Not supported.
		Call received from a trunk that is not programmed to provide release supervision.	None. Not supported.
			Page 2 of 2

Features C

Table 27: Troubleshooting Features

Feature	Symptom	Probable Cause	Corrective Action
Call Forwarding	Unable to forward call between two internal phones.	Forwarding station and the destination station are not allowed to call each other.	Ensure that the forwarding station and the destination station are permitted to connect to one another in Interconnect Restriction Table.
	Cannot forward calls to a tenant.	One or both tenants do not have permission to call each other (that is, each tenant has granted the other tenant calling permission).	Program both tenants to allow them to call each other. See Tenanting in the System Administration Tool online help information on tenant permissions.
	CFFM or Call Forward - No Answer not behaving as expected.	Set is a member of a Hunt Group. The options for CFFM and Call Forwarding are set differently in the Hunt group COS than the COS of the set.	The Hunt Group COS (or, if no Hunt Group COS is programmed, the COS of the first member of the Hunt Group) is used for the following COS options: • Call Reroute after CFFM to busy destination • COV/ONS/E&M Voice Mail Port • ONS/OPS Internal Ring Cadence for External Callers (only if the first member is ONS/OPS) • ANSWER PLUS - Delay To Message Timer • ANSWER PLUS - System Reroute Timer • Call Forward - No Answer Timer
	Call forwarding not functioning on a 5320, 5330 5340 or 5360 IP Phone.	User tried to program Call Forwarding using the **Superkey**.	Use the Call Forwarding application to program call forwarding on the 5320, 5330, 5340 and 5360 IP Phones.
	IP Set is forwarded to other destination for no apparent reason. "Locate Feature Extension" maintenance command from ESM does not show call forwarding active.	Call forwarding set up from associated Your Assistant application via Mitai event. MCD cannot detect and identify this type of call forwarding features using "Locate" mainteance command.	If the call forwarding is no longer valid or required, disable it for the IP set via YA.
			Page 1 of 4

Table 27: Troubleshooting Features

Feature	Symptom	Probable Cause	Corrective Action
Call History	Calls not being logged.	The following calls are not logged by the Call History feature: • incoming ACD Calls and Personal calls from ACD agents • calls to non-prime broadcast groups • calls to a device that is forwarded/rerouted to “Always”.	None. Not supported.
	Unable to place calls to external numbers that are stored in your Call History list.	Outgoing prefix is required to dial the external number from Call History.	If you have programmed a specific Call History feature button on the person's phone, you can add the prefix digits using the option “Outgoing External Call Prefix For Applications” in the System Options Assignment form. **Note:** This solution does not work if Call History is accessed via the Superkey/Blue button on the phone. Also see Table 16, “Specific Model Troubleshooting,” on page 59, and if the problem is seen on 5235 IP Phones.after failover, see Table 56, “Troubleshooting Sharing Operations,” on page 168.
	Caller name not displaying in Call History on 5140/5240 set for calls comes from NI-2 5ESS PRI.	Caller name not in the protocol message required by these sets.	None. Not supported.
Call Pickup - Directed	Users cannot pick up calls from a set.	Class of Service option “Call Pickup - Directed: Accept” is not set to “Yes”.	Set “Call Pickup - Directed: Accept” to “Yes” in the Class of Service of the ringing set.
	User unable to pick up calls from Attendant Console.	Class of Service option “Allow Directed Call Pickup of Attendant Call“ not enabled.	Enable “Allow Directed Call Pickup of Attendant Call” in the Class of Service Options form of the user’s set.

Table 27: Troubleshooting Features

Feature	Symptom	Probable Cause	Corrective Action
Call Pickup - Clustered	Remote elements that host the clustered call pickup group are not updated with a directory number change after an SDS synchronization. An SDS updates error is generated in the System Administration Tool to alert you that the change was not made on the remote elements.	You must remove a member from a clustered pickup group, before you change the member's directory number; otherwise the remote elements that host the clustered call pickup group will not be updated with the change by an SDS synchronization.	Refer to the Call Pickup -Clustered topic in the System Administration Tool online help for instructions.
Camp-on	Unable to camp-on to a group.	Maximum number of allowable camp-ons to a group is exceeded.	Try again at a later time. The maximum number of camp-ons to a group per 3300 ICP is set at 84.
Clear All Features	Feature not cancelled by code.	"Clear All Features" code does not cancel all features. It will not cancel: • Hold (any type) • Account Codes (voice or data) • Rerouting • Callbacks set against your station • Message waiting notifications.	Ensure that the "Clear all Features" code supports the cancellation of the set feature.
Conference	Unable to establish join a conference.	The maximum number of callers in a single conference (maximum of 8) has been reached	Refer to the Conference feature in the System Administration Tool online help for the conference limitations for your 3300 ICP controller.
	Unable to establish a conference.	Maximum number of conferences that you system can support has been reached	
	Cannot make conference call from single line set.	If COS option Call-Waiting Swap is enabled, user cannot make conference call from single line set. This is because Call-Waiting Swap overrides the conference feature.	Disable Call-Waiting Swap in the COS.
	Cannot create a conference between two external PSTN callers.	Incorrect Calling Line Identification (CLID) is being sent to third party.	Enable "Replace External CLID" in ISDN Protocol form of trunk.

Table 27: Troubleshooting Features

Feature	Symptom	Probable Cause	Corrective Action
Conference Split	Unable to split a conference call.	Split cannot be activated from a telephone when: • the attendant is involved in the conference • a member of the conference has a party on Consultation Hold • the conference is on Hold • a member of the conference has a party camped-on • members of the conference belong to the same Key System Group • you are in select features or display mode • there are more than three members in the Conference.	Ensure call conditions support the Conference Split feature.
			Page 4 of 4

Features D to G

Table 28: Troubleshooting Features D to G

Feature	Symptom	Probable Cause	Corrective Action
Direct Page	Phone user did not receive a Direct Page.	Handsfree Answerback is only available on some phones.	Only phones with a built-in speaker can receive one. See The Phone -Feature Availability matrix in the System Administration Tool online help for more information.
		IP Phone user is on a call on the analog line of the Line Interface Module.	Ensure analog line of Line Interface module is not in use at the time of the page.
		The paged phone has a call on soft hold (i.e. transferring a call).	Ensure paged phone was not on soft hold when page was initiated.
		The paged telephone is engaged in a handsfree call.	Ensure user was not engaged in a handsfree call when the page was made.
		The user of the paged telephone is dialing a number when the Direct Page is received.	Ensure user was not dialing a number when the page was made.
	User hears reorder (busy) tone when attempting a direct page,	The IP page group has exceeded the maximum limit of 64 IP devices.	Reduce the number of IP-device members to 64 or less.
		One or more IP sets has reset during paging setup.	Ensure that none of the sets that you attempted to page are in the process of being reset.
			Page 1 of 3

Table 28: Troubleshooting Features D to G

Feature	Symptom	Probable Cause	Corrective Action
DSS/BLF key	Cannot program a DSS/BLF key.	You are trying to assign a directory number that does not already exist in the system.	Add the directory number in the Telephone Directory form before you assign the DSS/BLF key.
	In a clustered environment, error logs related to the DSS/BLF keys are being generated at the remote system.	The programming on the remote system is not complete.	Check that the DSS/BLF keys are programmed in the Remote Busy Lamps form on the remote system. If not, complete the DSS/BLF key programming on the remote system. See the Direct Station Select/Busy Lamp Field feature in the System Administration Tool online help for instructions.
	In a clustered environment, the button is not showing the person's status/	The Remote Host Set Directory Number is not listed in the Remote Busy Lamps form on the MCD of the monited extensions.	On the MCD hosting the monitored extension, navigate to the Remote Busy Lamps form, and add the Remote Host Set Directory number.
	Phone is not ringing for entire ring cycle when a DSS/BLF key is used to place the call.	DSS/BLF key set to **Ring** which provides single burst ringing.	In the Multiline Set Keys form, set the DSS/BLF key to **Ring Cont**.
Do Not Disturb	Call rings set when DND enabled.	The calls are incoming external calls. Do Not Disturb (DND) only stops internal calls from ringing a user's telephone and returns busy tone to the caller.	None. Feature functioning correctly.
Embedded Unified Messaging (UM)	Feature not working system-wide.	Programming incomplete. Embedded UM must be provisioned at the user level in the VM Mailboxes form and at the sytem level in the Embedded UM Settings form.	Complete the required programming.
Feature key	Feature key programmed on set but it doesn't enable the feature.	For a feature key to function, you must complete the required programming for the specified feature. For example, for the DND feature key to function, you must program the DND feature through the System Administration tool forms.	See the System Features book in the System Administration Tool online help for feature programming.
			Page 2 of 3

Table 28: Troubleshooting Features D to G

Feature	Symptom	Probable Cause	Corrective Action
Group page	Phone in Page Group does not receive page.	System restrictions prevent the phones from connecting with each other.	Ensure that COR and interconnect restrictions allow the paging and paged parties to connect.
		Number of supported IP Phones in the page group has been exceeded.	Ensure system has adequate resources to support paging requirements. Refer to the Engineering Guidelines for details
		Insufficient E2T resources to support the number of IP Phones.	
Groups - Key System and Multicall	Incoming call to Multicall Group does not ring Multicall line key on 5560 IPT.	The 5560 IP Turret cannot be a member of a Multicall group even though it can be assigned a Multicall line key in the Multiline Set Keys form.	None. Not supported.
			Page 3 of 3

Features H to K

Table 29: Troubleshooting Features H to L

Feature	Symptom	Probable Cause	Corrective Action
Handset Receiver Volume	Handset receiver volume setting is not retained between calls.	“Handset Volume Adjustment - Saved” option is not enabled for the set	Enable “Handset Volume Adjustment - Saved” option in the COS of the set.
Handsfree Operation	Called party cannot hear you clearly.	Microphone is obstructed	Ensure that the microphone (on the front edge of the telephone) is unobstructed
		Background noise	minimize background noise (such as printers, fans, and radios)
		Too far away from phone	sit within reach of the telephone
		Speaking too quietly	speak at a normal volume towards the microphone.
Hold	User unable to place DID On-Hold.	Users unable to put DID calls on hold when the COS of the set has Record-A-Call - Save Recording on Hang-up enabled.	Disable “Record-A-Call - Save Recording on Hang-up” option in the COS of the set.
Hunt Groups	Calls not ringing sets in expected order.	Incorrect “Hunt Group Mode” specified.	Ensure that the desired Hunt Group Mode (Circular or Terminal) is specified in the Hunt Groups form.
		Hunt group members are programmed in the wrong order in the Hunt Groups form.	Ensure that the member directory numbers are entered (listed) in the Hunt Groups form in the order that you want the calls distributed.

Features L to O

Table 30: Troubleshooting Features M to O

Feature	Symptom	Probable Cause	Corrective Action
Language Change	Selected language not appearing correctly on 5235 IP Phone.	There are exceptions for some languages on the 5235 IP Phone.	None. Review the conditions described in the System Administration Tool online help under the Language feature.
Loudspeaker Paging	Unable to perform loudspeaker paging	Attempting to perform Loudspeaker Paging feature in handsfree mode.	None. Loudspeaker Paging feature is not supported in handsfree mode.
Message Waiting Indication	The MWI lamps on ONS sets fail to light when a message is left even though the circuit descriptor is configured to provide MWI.	Programming incomplete or incorrect.	1. Verify that the circuit is assigned an ONS/OPS Circuit Descriptor that has the Message Waiting Lamp field on set to “Yes” 2. Verify that CLASS/CLIP phones have a Class of Service with the ONS CLASS/CLIP Message Waiting field set to “Yes.” 3. Verify that non-CLASS/CLIP phones have a Class of Service with the ONS CLASS/CLIP Message Waiting field set to “No.”
	In a network of PBX platforms, where stations are programmed to have voice mailboxes off of a Message Server or Speech Server application that is centrally located at a main site, the MWI fails to show the presence of new messages at the stations.	After the System Option “Superset Callback Message Cancel Timer” expires, MWI is disabled. This timer is expiring before the message is noticed.	In a network of PBX platforms, where stations are programmed to have voice mailboxes off of a Message Server or Speech Server application which is centrally located at a main site, the System Option, “Superset Callback Message Cancel Timer” must be programmed to “blank” on all remote site PBX platforms. Otherwise, the MWI will be disabled once this timer expires.
			Page 1 of 2

Table 30: Troubleshooting Features M to O

Feature	Symptom	Probable Cause	Corrective Action
Music on Hold	No music	Incorrect file format.	Save file in the following format: WAV, A-law or m-law (G.711), 8 kHz, 8-bit, mono.
		File too large.	See System Audio Files Update in the System Administration Tool online help for the maximum size of the audio files.
		In MCD 4.x+ Need to have ENABLE_TX_CHAN_CONN feature enabled.	Refer to Mitel Knowledge Base article 11-5160-00010. **Note**: This feature is available only on MCD 4.x and above.
	Distortion	.WAV file conversion introduced distortion.	When extracting a file from a CD (for a example, from your corporate Music on Hold CD) using a “CD ripper” application, choose a sampling rate as close as possible to 8 kHz. This should help prevent audio distortion introduced when converting a WAV file from a high sampling rate to a low sampling rate.
	Music on Hold (MOH) via ASU becomes garbled or develops static after approximately 2 to 3 weeks in service.	Hardware problem with the Universal ASU (P/N=50001266).	Update the revision of the Universal ASU to A16 or B4 though the standard repair process. The normal repair warranty is in effect. **Note:** For a temporary work around, reset the ASU. This will clear the problem for a couple of weeks.
	Cannot download Audio Files to the 3300 ICP	The audio file cannot be located.	Verify that the audio file is not corrupted.
		The audio file is rejected.	Verify that the audio file meets the required specifications (see System Audio File Updates form).
		The system greeting audio file is in the wrong language.	Download a file in the correct language using the System Audio File Updates form or Enterprise Manager (see your Mitel dealer for information on Enterprise Manager).
		A system error log is generated.	Verify that you are not attempting to download a file during a backup, restore or upgrade, or while somebody is recording the same greeting from a phone.

Features P to R

Table 31: Troubleshooting Features P to R

Feature	Symptom	Probable Cause	Corrective Action
Private Line Automatic Ringdown (PLAR)	Feature not functioning.	PLAR is only configured at one end of the connection	Configure PLAR in the same manner at both ends of the connection.
		One or both systems have pre- 3300 Release 8.0 software	Support for PLAR on E1 links is limited to systems with Release 8.0 or higher software. Upgrade systems to Release 8.0 or later.
Record a Call	Feature not available.	Advanced Voice Mail option not enabled. Record-A-Call requires the Advanced Voice Mail purchasable option.	Purchase and enable Advance Voice Mail option.
Ring Groups	Calls to group not overflowing to programmed call overflow destination directory number.	The directory number programmed as the overflow destination is invalid (unsupported directory number).	Program the ring group's overflow destination with a directory number from one of the following: • station DNs • broadcast group DNs • attendant console DNs • system speed call number • hunt group DN • ring group pilot DN

Features S to V

Table 32: Troubleshooting Features S to V

Feature	Symptom	Probable Cause	Corrective Action
Telephone Directory Support	After exporting data to a Microsoft Excel spreadsheet, you are unable to open the spreadsheet.	PC settings require modification to allow file to be launched.	To launch Excel Spreadsheets • Disable the pop-up blocker in your browser. • In Windows Explorer, click **Tools > Folder Options**. • Click the **File Types** tab. • In the **Registered File Types** list, select the XLS Microsoft Excel Worksheet type. • Click the **Advanced** button. • Clear the **Browse in same window** box. • Check the **Confirm open after download** box. • Click **OK**, and then click **Close**.
Transfer	Call cannot be transferred to an internal party.	Interconnect Restrictions prevent the two parties from connecting.	Modify Interconnect Restriction form to allow the two parties to connect.
Trunk Answer from any Station	Station user cannot pick up incoming call ringing at Night Bell directory number.	Interconnect Restrictions preventing station user from accessing incoming trunk.	Ensure that TAFAS stations have access to the incoming trunks in the Interconnect Restriction Table.
Speed Call - Pause	Dialing error occurs when using a speed call that is programmed with a pause. The digits proceeding the Pause are processed but the digits after the Pause are not because the Inter-digit Timer expires before the Pause.	Pause in Speed Call is longer than the Inter-digit Timer:	Shorten the length the pause or increase the Inter-digit Timer in the Class of Service of the trunk.
Speed Call - Personal	User cannot store speed calls against index numbers.	User is trying store speed call number against single digit Index numbers. Index numbers must be two-digit numbers within your assigned range (00 to a maximum of 99).	When storing personal speed calls against index numbers, For numbers 0 to 9, add a leading zero. (For example, 00, 01, 02, 03 and so on).

CHAPTER 6

TRUNKING

Trunk Troubleshooting Tips

- ☑ If all the circuits supported by a module or card are out of service, it is likely defective. If possible, swap the module or card with a known working module or card to confirm.
- ☑ For help with *diagnosing* trunk problems, see “Trunks” on page 209.
- ☑ In the System Administration Tool, use the
  - Line Quality Measurement Tool to test Loop Start Trunks that are connected to the AX Controller Card Chassis, Analog Main Board, Analog Option Board, or ASU II.
  - Voice Quality Statistics form in combination with NetAlly (must be purchased separately) to identify voice quality problems and performance trends for IP phones.

Analog Trunks

Table 33: Troubleshooting Analog Trunks

Symptom	Possible Cause	Corrective Action
System not receiving trunk calls.	Analog trunk issues.	Verify that the analog trunk is OK by using individual trunk access and testing on the frame.
	.Answer point not programed.	Verify SMDR records to see which trunks have received incoming calls. Verify that the answer point is programmed correctly and is functional.
Outgoing calls are dropping after a couple of minutes into the conversation.	The system is not receiving answer supervision from the central office and is timing out.	If the Central office cannot provide answer supervision on answered calls go to the CO Trunk Circuit Descriptors form and change the value in the field ”fake answer supervision after outpulsing” to yes.
Unable to dial out on trunk.	No dial tone	Ensure dial tone is present from Central Office (CO). You can disable dial tone detection on the trunk to allow users to dial out on the trunk in the absence of dial tone.
Calls are connecting to the far end. Called party can hear caller, but calling party cannot hear party at far end.	The system is not receiving answer supervision immediately from the Central Office.	Go to the CO Trunk Circuit Descriptors form Change the Supervision parameters in the value field “audio inhibit until answer supervision after outpulsing” to No.
Trunks are programmed but are appearing as unassigned with the STAT location ID command.	Card has not had the information downloaded to update the status of the trunks.	Download the information to the ASU at an appropriate time.
		Page 1 of 3

Table 33: Troubleshooting Analog Trunks

Symptom	Possible Cause	Corrective Action
Ring is not heard immediately when external phone calls on LS trunk.	An external phone that is connected to the LS trunk rings four times before the receiving phone rings. When the class of service option ANI/DNIS Delivery Trunk is enabled, the system waits for the ANI information before making the phone ring. If this is not provided, the phone will not ring immediately.	In the COS of the LS trunk, disable **ANI/DNIS Delivery Trunk**.
Poor audio quality on LS trunks	Incorrect country loss level plan.	In the License and Option Selection form, ensure that the Country field is set correctly for the system. The Country setting determines the default language, dialing plan, tone plan, and loss and level plan for the system. Refer to the Hardware Technical Reference Manual for tables that list the Loss Level Plans. You can also check with the Mitel Regional Sales office to find out the most appropriate setting for your region.
	Incorrect Balanced Network Setting or Trunk Category in the Trunk Circuit Descriptor form for the trunk.	Use the Line Quality Measurement tool in the System Administration Tool to determine the correct settings.
	Inadequate system grounding	Ensure that the “Protective Ground” on the rear panel of the controller, ASU, or Peripheral Cabinet is connected to a solid ground. Refer to Appendix B in the Hardware Technical Reference Manual for additional grounding information.
Poor audio quality occurring intermittently on LS trunks.	If incoming calls arrive from trunks that are members of a trunk hunt group, an audio quality problem on a trunk in the group will appear as an intermittent problem on the phones.	Use the Line Quality Measurement tool in the System Administration Tool to check the settings of each LS trunk in the hunt group.
	Caller is using a cell phone that does not support the International Telephone Union (ITU-T) recommendation for the Send Loudness Rating (SLR).	If the caller is using a cell phone that has a low SLR, a user on the system will receive low audio. This is an issue with the caller’s cell phone.
		Page 2 of 3

Table 33: Troubleshooting Analog Trunks

Symptom	Possible Cause	Corrective Action
Poor audio quality on LS trunks on the 3300 ICP MX, CX, or CXi platforms.	Not utilizing latest DSP enhancements.	To improve audio quality on LS interfaces used on the 3300 ICP MX, CX, and CXi platforms, a new technology and DSP enhancement was introduced in 3300 Release 6.1 UR1 (6.1.7.11_4). This product enhancement addresses the following audio quality issues: • Echo at the beginning of outgoing calls via the LS interface on the AMB and AOB boards. • Double-talk or choppy audio when internal party speaks at the same time as the external party. Upgrade the 3300 ICP to Release 6.1.7.11_4 or later. Then, re-run the Line Measure Tool on the embedded analog trunks. The recommended settings suggested by the LS Measure tool must be programmed in the trunk circuit descriptors to activate this echo canceller enhancement. This enhancement applies only to the embedded analog trunks. **Note**: Set the trunk circuit to LONG before running the Line Measure Tool. This setting is crucial when using internal milliwatt tone, instead of the Telco's milliwatt tone.
Poor audio quality on LS Trunk on a UK site.	Incorrect subscriber line has been provided by the carrier.	To ensure that the correct lines are provisioned in the UK, ensure that the Telco (e.g. BT), or carrier, provides trunks that are compatible to System X line type ‘0’ (Subscriber lines) or line type ‘3’ (business PBX/PABX lines). Both types of lines will work satisfactorily with the 3300 ICP, however line type ‘3’ is the preferred line type for connecting a PBX/PABX.
LS Class trunk fails to display or collect Calling Line Identification (CLID) on the embedded ASU in a 3300-MX controller.	The **ANI/DNIS/ISDN Number Delivery Trunk** option is enabled in the COS of the trunk. When this option is enabled, the LS class trunk fails to collect CLID during the first and second ring cycle and only the trunk label will be displayed on the set. If this option is enabled, it takes an additional 5 to 12 seconds before the call is presented to the set.	Disable the **ANI/DNIS/ISDN Number Delivery Trunk** option in the COS of the trunk.
		Page 3 of 3

Digital Trunks

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
General		
Excessive Bit Error Rate.	Faulty programming.	Make sure the system is programmed the same as the CO, for B8Zs or AMI
Excessive Slips.	Faulty programming.	Ensure the Network Synchronization form is programmed and the system is clocking appropriately. Use the Netsync Summary maintenance commands to determine if synchronization is taking place, If not, use Net Set 1 to set off the first clock source or NET SET AUTO to select the best available clock source. After you choose a synchronization clock source always use the NET SET AUTO command to confirm.
System is not Receiving Calls.	The DID trunk digit modification number on the Trunk Attributes form does not have anything programmed in the absorb field. It MUST have a minimum of 0, or no calls will be accepted.	Ensure that there is an entry in the absorb field. It cannot be left Blank.
	Faulty ANI/DNIS programming.	Check ANI/DNIS programming to ensure there has not been confusion with a DID trunk. For ANI/DNIS to work the digit must be received from the Central Office as *ANI*DNIS*. If the digits are not being received in this format, turn off the ANI/DNIS in the Class of service Options.
Outgoing calls are dropping after a couple of minutes into the conversation.	System is not receiving answer supervision from the central office and is timing out.	If the Central office cannot provide answer supervision on answered calls go to the CO Trunk Circuit Descriptor Assignment and change the value in the field ”fake answer supervision after outpulsing” to Yes.
Calls are connecting, and the far end can hear us but we cannot hear them.	System is not receiving answer supervision immediately from the Central Office.	In the CO Trunk Circuit Descriptors form, change the Supervision parameters in the value field “audio inhibit until answer supervision after outpulsing” to No.
Trunks are programmed but are appearing as Unassigned with the STAT location ID command.	Card has not had the information downloaded to update the status of the trunks.	Download the information to the NSU at an appropriate time.
		Page 1 of 7

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
T1 Trunk unstable or 3300 ICP resets or both.	Improper cable. Cat 5 Ethernet Cable for PC is not approved to use as a standard RJ45/T1 cable.	Use shielded R45-R45 T1 cable for T1, ISDN line and/or DSU/DSU connections. Without proper shielded pairs, the signal integrity on a T1 trunk is not guaranteed. Refer to Mitel Knowledge Base article 08-5191-00123 for additional details.
T1 E&M trunk call cannot be transferred or put on hold.	Release Link Trunk (RLT) setting in the Trunk Attributes form is set to YES. This setting is only intended for T1 integration to centralized attendant. If the RLT field is set to YES for normal operation, it will cause these symptoms.	For normal T1 E&M trunks, set the RLT field in the Trunk Attributes form to NO.
Incoming T1 E&M trunk call limited to 10 digits. (Affects applications such as fax servers trying to dial numbers over 10 digits--e.g., long distance calls).	Trunk COS has "ANI/DNIS/ISDN Number Delivery Trunk" option enabled which limits the maximum number of incoming digits to 10. With option disabled, the trunk can receive more than 10 digits.	Set "ANI/DNIS/ISDN Number Delivery Trunk" option to "No" in the trunk COS.
NSU does not come into service after you change links from T1 to E1 or vice versa.	The NSU failed to download the new virtual Digital Service Unit (VDSU) files from the controller.	Enter the “force dl” command from the NSU maintenance port. This command causes the NSU to reboot and get the proper VDSU files. The NSU maintenance port is set for 38400 baud rate, 8N1 parity
External forwarding of an incoming PRI call is not successful.	The COS of the incoming PRI does not allow Public-to-Public trunk connection.	In the COS of the incoming PRI trunk, enable “Public Network to Public Network connection allowed”.
	There is a COR restriction against the incoming PRI trunk in the ARS route.	For COR restriction, ensure the COR number of the PRI trunk is not included in the COR group defined for the specified route in the ARS Routes form. See the document “Using CDE to Prevent Toll Fraud on the 3300 ICP” for more information. This document is available in the 3300 ICP System Administration Tool online help.
	Q.Sig Private network access is enabled in PRI link descriptor.	For the link descriptor assignment used by the PRI link, set “Q.Sig Private network access” to NO. (This option should not be enabled for normal PRI. It should only be set if the link is intended for Q.Sig.)
After you install or initially program an embedded E1 module, the DASS II link does not work.	In the Link Descriptor Assignment for the DASS II link, the CRC-4 is set to “Yes”.	In the Link Descriptor Assignment for the DASS link, set the CRC-4 setting to “No” and then reset the controller. If you alter the CRC-4 setting, you MUST reset the controller to enable the new, or changed, setting.
		Page 2 of 7

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
DASS II circuit fails to return to service after programmed reboot.	The MN 3300 NSU. takes approximately seven minutes to come back after a programmed reboot. The service provider has a threshold of only five minutes, after which they will take the link out of service.	Refer to Mitel Knowledge Base article 04-3849-00502.
Cannot dial international numbers when connected to DMS500 switch running DMS100 protocol.	System is connected to a DMS500 switch running DMS100 NI1 protocol and the service provider has an NI2 table programmed in the central office. The protocol may set correctly in the central office; however the NI2 table should not be programmed.	Refer to Mitel Knowledge Base article 05-5107-00005.
DID call with number in the name portion fails to access Auto Attendant directly.	Inbound ISDN calls which present numbers in the name portion of the call will not complete. The voice mail which uses screen scrapes are seeing the numbers in the name portion of the caller as choice or extension number, instead of a trunk call, As a result, the DID caller does not hear the auto attendant greeting and may hear other voice mail option or “please enter your mailbox number prompt”.	In the voice mail port's class of service, set the following: • display ani/isdn calling number only YES • display ani/dnis/isdn calling/called number YES.
The 3300 ICP is inter-operating with a Tenovis PBX via a Q.Sig trunk. A station on the Tenovis PBX is unable to display the CLID of an incoming call.	The 3300 ICP is the transit PBX and is running a software version that is earlier than 3300 Release 7.0 UR2. Both Mitel and Tenovis follow the Q.Sig specification but they use different options. This is an interoperability issue between the two systems.	Upgrade to 3300 Release 7.0 UR2 or later. In addition, the following programming is required: For an embedded NSU with Release 3300 7.0 UR2 or later software: 1. Access the System Administration Tool on the 3300 ICP. 2. Select the ISDN Protocol form. 3. Enter “ctcomplete” in the comment field of the ISDN Protocol form for the corresponding Q.Sig link. For a NSU with 3300 Release 7.0 UR2 or later software 1. Access the IMAT tool. 2. Select the PRI link characteristics. 3. Enter “ctcomplete” in the comment field. Ensure that you save the changes in the NSU.
		Page 3 of 7

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
Outgoing call on PRI E1 trunk (using Euro ISDN protocol) to a busy PSTN (number is dropped instead of receiving busy tone.	Link using Incorrect protocol variant.	**3300 ICP Release 4.0 - 5.1** Upgrade to Rel 5.1.4.8 and set Euro ISDN Protocol Variant as explained below **3300 ICP Release 5.1.4.8 and higher** Set Euro ISDN Protocol Variant as explained below For the Network Service Unit (NSU), set the Protocol Variant via IMAT as follows: 1. In IMAT System Configuration, select PRI Link Characteristics. 2. Under Protocol Variant for Euro ISDN, select Telecom Italia. 3. Save the database back to the NSU or PRI (and reload the NSU when convenient.) For embedded T1/E1, set the Protocol Variant via ESM as follows: 1. Log into the System Administration Tool 2. From the Selection menu (alphabetical view), choose ISDN Protocol. 3. Highlight the module required, and change to Telecom Italia under Protocol Variant for Euro ISDN.
No ANI displayed when call is transferred over Q.SIG from Mitel system to foreign PBX.	ANI missing from the CTCOMPLETE facility message in the Q.SIG signaling.	Add “ctcomplete” to the Comment field in the ISDN Protocol Assignment form in ESM. (Omit the quotation marks.)
Embedded PRI		
Embedded PRI calls fail and all Status LEDs on the Dual T1/E1 Framer are OFF.	Configuration.	Verify that embedded PRI is programmed properly in the following forms (see also Program Embedded PRI/Q.SIG in the Online Help): • Controller Module Configuration • Dual T1/E1 Framer Configuration • Link Descriptor Assignment • Digital Link Assignment After the Digital Links form is completed, the T1/E1 Framer status LEDs should come on. This takes about 15 seconds.
Embedded PRI Links are “not seizable”, Status LEDs show RED alarm.	Configuration or wiring.	Ensure that the ISDN cable is plugged into the correct RJ-45 port on the Dual T1/E1 MMC. Verify that the ISDN cable is correctly wired. Change the “Termination Mode” setting in the Digital Link Descriptors form - either LT or NT. This change takes about 30 seconds to take effect.

Page 4 of 7

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
Embedded PRI links are “not seizable”, Status LEDs show flashing GREEN.	Configuration.	Verify the “Network Side/QSIG Master” setting in the ISDN Protocol form. Check the “Inverted D-Channel” setting in the Digital Link Descriptors form - normally it is set to “No”. Each of these changes takes approximately 30 seconds.
Embedded DPNSS links are “not seizable”, Green LED is ON	Configuration.	Ensure that the “Address for Message Control” field in the Digital Link Descriptors form is set appropriately (“A” or “B” depending on the far end. If the configuration is correct, wait for about one minute until every circuit has finished negotiation with the far end.
Distorted voice or loud noise over PRI/QSIG call	Voice Encoding is not set properly.	In the Link Descriptor Assignment for the PRI/QSIG trunk, set the “Voice Encoding” to Nil for T1 on NA or E1 on Euro controller. Note: You cannot use the same Voice Encoding settings as a PRI NSU.
High number of slips.	Configuration of Network Synchronization form.	Ensure that the synchronization source being selected is to a digital PSTN trunk (like PRI or T1/D4).
Outgoing calls fail with reorder tone.	Configuration error in ARS programming or ISDN Protocol form.	Enter the CCS TRACE maintenance command to ensure that the proper digits are being sent out. Check the Digit Modification with the Per-Call programming for PRI to make sure digits are not being inserted or absorbed unnecessarily. Ensure that the “Protocol” field in the ISDN Protocol form is correct for the PSTN link (not for DPNSS).
Incoming calls fail.	Configuration error in Trunk forms.	Verify in the Trunk Attributes form that there is an Answer Point set up for non-DID trunks for Day and Night services. For dial-in trunks, verify that the “Dial in Trunks Incoming Digit Modification - Absorb” field is set to 0 and that the “Dial In Trunks - Incoming Digit Modification - Insert” field is set appropriately for dial in trunks.
Access denied when calling out on a PRI trunk.	Programming error.	PRI and MSDN trunks are considered to be DPNSS by the system. The Class of Service (COS) option “Public Network Access via DPNSS” of the dialing device must be set to Yes. (The default is No).
When dialing out on a PRI trunk the call is connected, however no audio path is established.	Programming error.	In Trunk Attributes form, ensure that Release Link Trunk is set to No.
		Page 5 of 7

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
Unable to forward an incoming PRI call to an external destination.External forwarding of an incoming PRI call may not be successful for one of the following reasons.	COS of the incoming PRI does not allow Public-to-Public trunk connection.	In the COS of the incoming PRI trunk, enable **Public Network to Public Network connection allowed**.
	COR restriction against the COR of the incoming PRI trunk in the ARS route.	For COR restriction, ensure the COR number of the PRI trunk is not included in the COR group defined for the specified route in the ARS Routes form. **Note**: You may need to refer to the Toll Fraud control document Knowledge Base Article # 04-1000-00060 “Using CDE to Prevent Toll Fraud on the MN3300 ICP”.
	Q.Sig Private network access is enabled in PRI link descriptor.	For the link descriptor assignment used by the PRI link, set **Q.sig Private network access** to **NO**. (This option should not be enabled for normal PRI, only if this link is intended for Q.Sig.).
Calls on PRI trunks do not present outbound name.	Not supported by protocol used on the PRI trunks. Outbound name is only supported by PRI trunks that use DMS-100 or QSIG protocols.	Refer to Mitel Knowledge Base article 05-3849-00988 for a list of the protocols that support outbound name.
QSIG ISO feature not functioning.	QSIG feature not supported. For unsupported QSIG features, the 3300 will not act as a transit switch.	See Mitel Knowledge Base article 06-5191-00064_1 for a list of the QSIG features supported on the 3300 ICP
Embedded BRI		
Embedded BRI calls fail and all Status LEDs on the Quad BRI Framer are OFF.	Configuration.	Verify embedded BRI is programmed properly in the following forms (see also Program Embedded BRI in the online Help): • Controller Module Configuration • Quad BRI Framer Configuration • Link Descriptor Assignment • Digital Link Assignment • Protocol Assignment After the Digital Links form is completed, the red Quad BRI Framer status LED should come on. This takes about 15 seconds.
Embedded BRI Links are “not seizable”, Status LEDs show RED alarm.	Configuration or wiring.	Ensure that the ISDN cable is plugged into the correct RJ-45 port on the Quad BRI MMC. Verify that the ISDN cable is correctly wired (straight through for trunk interface, crossover for terminal). Note that 3-4 and 5-6 are the relevant pins for the cable. Toggle the “Bus Type” setting in the Protocol Assignment (either S or T). This change takes about 30 seconds to take effect. Ensure that the Manual TEI value is correct (if required).

Table 34: Digital Trunk Troubleshooting

Symptom	Probable Cause	Corrective Action
High number of slips.	Configuration of Network Synchronization form.	Ensure that the synchronization source being selected is not connected to a BRI terminal. If there is a digital E1 trunk, that should be used as the first synchronization choice.
Outgoing calls fail with reorder tone.	Configuration of ARS or configuration of Per Call Capabilities.	Enter the CCS TRACE maintenance command to ensure that the proper digits are being sent out. Check the Digit Modification with the Per-Call programming for BRI to make sure digits are not being inserted or absorbed unnecessarily.
Incoming calls fail.	Configuration of Trunk forms.	Verify in the Trunk Attributes form that there is an Answer Point set up for non-DDI trunks for Day and Night services. For dial-in trunks, verify that the “Dial-in Trunks Incoming Digit Modification - Absorb” field is not left blank and that the “Dial In Trunks - Incoming Digit Modification - Insert” field is set appropriately for dial-in trunks.
R2 Line Signaling		
R2 setup issue	Programming or installation	Refer to Mitel Knowledge Base article 05-5191-00050.
		Page 7 of 7

MSDN/DPNSS Links

Table 35: MSDN/DPNSS Link Troubleshooting

Symptom	Probable Cause	Corrective Action
Embedded MSDN/DPNSS calls fail and all status LEDs on the T1/E1 MMC are OFF.	Faulty configuration.	Verify embedded MSDN/DPNSS is programmed properly in the following forms: • Controller Module Configuration • Framer Configuration –> T1/E1 Framer Configuration • Link Descriptor Assignment • Digital Link Assignment After the Digital Links form is completed, the red T1/E1 MMC status LED should come on. This takes about 15 seconds.
Embedded MSDN/DPNSS links are “not seizable” and the red LED is ON.	Faulty configuration or wiring.	Ensure that the T1/E1 cable is plugged into the correct RJ-45 port on the T1/E1 MMC. Verify that the T1/E1 cable is correctly wired. Note that 1&2 and 4&5 are the relevant pins for the cable. Toggle the “Termination Mode” setting in the Link Descriptor Assignment (either NT or LT). This change takes about 15 seconds to take affect.
Embedded MSDN/DPNSS links are “not seizable” and the green LED is ON.	Faulty configuration.	Ensure that the “Address for Message Control” field in the Digital Link Descriptors form is set appropriately (either “A” or “B” depending on the far end). If the configuration is correct, wait for about 1 minute until the every circuit has finished negotiating with the far end.
High number of slips.	Incorrect configuration of Network Synchronization form.	Ensure that the synchronization source being selected is to a digital PSTN trunk (like PRI or T1/D4).
User is unable to make an MSDN link call.	Programming error in Trunk Attributes form.	Ensure that the Trunk Attributes form is programmed correctly **at both ends** of the link. Specifically, dial-in trunks must have an entry in the Absorb column. (Enter '0' if no digits are to be absorbed.) For example, if the Trunk Attributes form of the Local system is programmed correctly but the form in the Remote system is **not** programmed correctly, MSDN calls will succeed only from Remote to Local. Calls made from Local to Remote will fail.
		Page 1 of 2

Table 35: MSDN/DPNSS Link Troubleshooting

Symptom	Probable Cause	Corrective Action
Outgoing calls links fail with re-order tone.	Faulty configuration in ARS.	Ensure that the proper digits are being sent out – get a “ccs trace” from the maintenance command window in ESM. Also review the routing of the call throughout the PBX network. Verify that the far end is ready to properly accept the call.
Incoming calls fail.	Faulty configuration of trunk Forms.	Verify in the Trunk Attributes form that there is an Answer Point setup for non-DDI trunks for Day and Night services. For dial in trunks, the “Dial In Trunks Incoming Digit Modification – Absorb” is not left blank and that the “Dial In Trunks Incoming Digit Modification – Insert” is set appropriately for dial in trunks.
All calls on a DS1 or CEPT card link fail.	Faulty cable connections, cable, or card.	Check the status of the link by using the DTSTAT READ PLID maintenance command. Check the cabling and cable connections. Test with a back-to-back cable to prove the DS1 or CEPT card. Replace faulty cable or card.
Only some calls on a DS1 or CEPT card link fail.	Configuration errors in programming • ARS programming error • Digit conflict • Interconnect Restriction preventing call • Far end fault/programming	Correct programming through System Administration Tool.
Only calls to the central office fail.	Faulty programming.	Ensure the Class Of Service option of “Public Network Access via DPNSS” is enabled on the extension making the call and the for MSDN trunks.
Cannot Group Page across MSDN trunks or IP trunks.	If one system has pre- 3300 Release 5.2.4.4 software and the other system has post-Release 5.2.4.4, the remote group page will fail due to incompatible signalling.	Upgrade all systems to Release 5.2.4.4 software or higher.
		Page 2 of 2

XNET

Table 36: XNET Troubleshooting

Symptom	Probable Cause	Corrective Action
Caller reports reorder tone when calling to another system.	Errors in the XNET ARS programming.	1. Ensure that the ARS Leading Digit Assignment and ARS Digits Dialed Assignment forms translate the dialed digits to an XNET route. Either the digits do not resolve to a route, or the route does not have the XNET Trunk Group Number field programmed. 2. Ensure that the PBX Number field in the IP/XNET Trunk Groups form contains a system number which exists in the XNET network. 3. Ensure that the PBX Number field in the IP/XNET Trunk Groups form contains a System number which is programmed correctly on the Local PBX: • The outgoing signaling DID number at the Local PBX must match the correct remote incoming list. • The outgoing voice DID number at the Local PBX must match the correct remote incoming list. • Interconnect restrictions must be set up incorrectly in the IP/XNET Trunk Profiles form on the Local PBX (the profile number must agree with the correct remote profile number, and must have the correct profile setting). 4. Ensure that the PBX Number field in the IP/XNET Trunk Groups form contains a PBX number that is correctly programmed on the Remote PBX: • The incoming signaling DID number at the Remote PBX may not match the correct local outgoing list. • The incoming voice DID number at the Remote PBX may not match the correct local outgoing list. • Interconnect restrictions may be set up incorrectly in the IP/XNET Trunk Profiles form at the Remote PBX (the remote profile number may not agree with the correct local profile number, or may be the wrong setting for the profile).
Caller reports busy tone when calling to another system.	Insufficient DID numbers allocated in the XNET ICP/PBX Networking form to set up voice channels to another PBX.	Allocate additional DID numbers.
		Page 1 of 2

Table 36: XNET Troubleshooting

Symptom	Probable Cause	Corrective Action
Call does not have the correct service profile.	Incorrect Local Profile Number.	Correct in the IP/XNET Trunk Groups form on the Local PBX.
	Incorrect Remote Profile Number.	Correct in the IP/XNET Trunk Profiles form on the Local PBX.
	incorrect Trunk Service Number or Interconnect Number.	Correct in the IP/XNET Trunk Profiles form on the Local or Remote PBX.
Signaling connection will not clear down or does not stay up.	Signaling Inactivity Timer fields are blank for the PBX pair in the ICP/PBX Networking form (blank at one or both of the systems).	Enter a value in the Signaling Inactivity Timer fields on both of the systems.
You cannot make XNET calls after a switch has been upgraded to a later version of software; for example, T37.6 or later.	Max Number of VoTDM Calls field in the XNET ICP/PBX Networking form is not completed.	Complete the Max Number of VoTDM Calls field in the XNET ICP/PBX Networking form.
One ore more of the following network features is not available: • IP Networking • XNET • Voice mail Networking	System Type is “Standalone”.	Program the System Type as “Enterprise” in the AMC.
		Page 2 of 2

IP Trunking (IP Networking)

Table 37: IP Trunk Troubleshooting

Symptom	Possible Cause	Corrective Action
IP trunk does not recover after router crash.	ICMP redirect is enabled.	1. On the RTC shell, use **routeShow** to identify the addition RouteHost entries, then use **routeDelete** to remove the entry. 2. For a permanent solution: • Make sure that the route has a “permanent” static route to the remote IP trunk network. • Turn IP redirect off. • Turn on the routing protocol between local router and ISP router.
Unable to place calls between systems via IP trunks in a clustered, redirected, or resilient environment.	PBX Number in the ICP/PBX Assignment forms of the systems are programmed incorrectly.	For each system in the cluster, ensure that the system’s PBX Number matches its CEID Index Number as defined in the Cluster Elements form.
Cannot Group Page across IP trunks.	If one system has pre- 3300 Release 5.2.4.4 software and the other system has post-Release 5.2.4.4, the remote group page will fail due to incompatible signalling.	Upgrade all systems to Release 5.2.4.4 software or higher.
Receive “out of service” tone while dialing across IP trunks to a remote element	Congested trunks at remote node. **Note**: this is not a local trunk congestion issue, the congestion is at the remote site. The remote site will have less trunks programmed than the originating site.	1. Launch the System Administration tool on the remote element. 2. Access the XNET ICP/PBX Networking form. 3. Increase Max Number of VOIP calls.

SIP Trunking

Table 38: SIP Trunk Troubleshooting

Symptom	Possible Cause	Corrective Action
When making a call in or out on SIP trunks the trunk number in the SMDR record is blank.	SMDR for SIP Trunks use the SMDR Tag field from the SIP Peer Profile form for the trunk number. If this field is blank, the trunk number in the SMDR record is blank.	Enter a Trunk Number (for example, 99) in this field and the number will be displayed as the trunk number in the SMDR record (for example, T099).

CHAPTER 7

TOOLS AND EMBEDDED APPLICATIONS

System Management Tools

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
System Administration Tool		
Unable to log into System Administration Tool, Group Administration Tool, Desktop Tools, or Visual Voice Mail phone application.	Database restore in progress	Wait for Database Restore operation to complete. Perform restores outside of business hours to minimize impact to users.
	Cookies are disabled in Internet Explorer or Firefox. All management tools depend on being allowed to set cookies to maintain session ID state, login fails if cookies are not enabled.	If the management tool fails to launch: **Internet Explorer** 1. Launch browser. 2. Select Internet Options from the Tools menu. 3. Select the Security tab and enable cookies. **Firefox** 1. Click on the Firefox button and then select **Options**. 2. Select the **Privacy** panel. 3. Set **Firefox will**: to Use custom settings for history. 4. Make sure **Accept cookies from sites** is selected. 5. Make sure **Accept third party cookies** is selected. 6. Click **Exceptions**.... 7. Make sure the MCD you're trying to access isn't listed. 8. If it is listed, click on its entry, then click **Remove Site**.
	Proxy server is enabled on your PC.	Disable proxy server in Internet Explorer (Tools, Internet Options, Connection, LAN settings).
Unable to log into System Administration Tool, Group Administration Tool, Desktop Tools, or Visual Voice Mail phone application.	5550 IP Console is running on Windows 98 operating system on the PC.	Close the 5550 IP Console application. The 5550 IP Console must be run as a standalone application on Windows 98 (that is, with no other application open while it is running).
		Page 1 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
The System Administration Tool displays a license violation message in one or more of the following formats: • Status banner in the top left corner of the System Administration Tool. • Pop-up during log in and log out. • Pop-up when forms are opened. • Pop-up when you are about to over-allocate licenses.	The controller is in license violation mode.	Correct the license violation event. Examples include: • License over allocation • Missing Designated License Manager • Missing Application Group Member • Core Package capability exceeded • License Keys cannot be validated • System ID mismatch • SDS is off (Enterprise System Type) • Duplicate System • Multiple Designated License Managers • Failure of timely synchronization with AMC • Application Group is in license violation mode • “licensekeys” or “licensecert” file has been corrupted
System Administration Tool unable to connect through Mozilla Firefox to MCD-ISS following reboot. Receive the following error: "Secure Connection Failed" Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number. (Error code: sec_error_reused_issuer_and_serial)	Browser cache conflict.	Clear Firefox cache: 1. Select **Options** > **Options**. 2. Click **clear your recent history**. 3. Under **Details**, ensure **Cache** is selected, and then click **Clear Now**. 4. Restart Firefox and attempt to reconnect to the MCD-ISS. If problem persists, switch to Internet Explorer 8 or higher.
The Group Administration Tool displays a license violation message when you log in or out.	The controller is in license violation mode.	Correct the license violation event.
“Script Error” Error Message, or a Dialog Fails to Appear	If the computer that you are using to access a MCD tool has pop-up blocker software installed, the administration tools (System Administration, Group Administration, or Desktop Tool) may not operate properly.	To access the administration tool or perform the administrative activity that the pop-up blocker software is preventing, you must allow pop-ups from the 3300 ICP to your PC.
		Page 2 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
Data Add/Change pop-up window fails to refresh in Firefox. After selecting URL in the window's Navigation Bar and pressing ENTER, a message sometimes appears saying "Please wait while the form is loading." Data may reload but pressing Cancel fails to dismiss pop-up (Cancel, Save, and Preview buttons also disabled).	Indeterminate.	Click **X** button in pop-up window to close. NOTE: You can prevent reoccurence by disabling the Navigation Bar via the Options menu in Firefox.
When you connect to the MCD tools for the first time from a client PC, you receive a warning that the site is not certified—for example: "There is a problem with this website's security certificate" (Internet Explorer) or "This Connection is Untrusted" (Firefox)	You need to install the trusted Mitel Root CA certificate on the client PC. If the web server is accessed by a URL not matching a DNS or local host filename in the certificate, your browser displays a warning that the name in the certificate does not match the name of the site. If the certificate is not installed, a security window is displayed. If using Internet Explorer, you must click **Continue to use this website (not recommended)** to proceed. Firefox users must click "**I understand the risks**" followed by **Add Exceptions**. Then, disable **Permanently store this exception**, and click **Confirn Security Exception**.	To stop these warnings from appearing, you must install the Mitel Root Certificate. The MCD System Tools login page contains a link to a help topic that provides instructions on how to download and install the Mitel Root Certificate.
The **Print Preview** function in the Print dialog of a System Administration Tool form fails. An error message similar to the following error is displayed: Line 48 Char 10 Object doesn't support this property or method https://10.40.131.17/uwi/pe/uwi_HiddenControllerPEWin.asp?Application=GenericForms&FunctionID=FI_Read&FunctionArgs	Internet Explorer on the client PC does not support 3300 ICP as a trusted site.	1. In Internet Explorer, click **Tools**, click **Internet Options**, click **Security**, and then click **Local Intranet**. 2. Click **Sites**, and then click **Advanced**. 3. Add the IP address of the 3300 ICP in the following format: https://<IP Address> 4. Click **OK** to close the dialog boxes.
		Page 3 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
System Administration Tool Online help is not available. When you click on the help buttons in the System Administration Tool, the help window displays “404 Page Not Found” error.	Web server that hosts the online help files is down.	Ensure web server is running.
Online help not appearing in System Administration Tool	Help not installed on external server or the path to the help is incorrect	Correct the path or install the help on the external server. See the System Administration Tool online help for instructions.
Non-Unique Match error when entering commands via the System Administration tool.	The busy command was entered and has not been completed. The system is waiting for further input (for example, FORCE) before executing the command.	Issue the FORCE command.
Receive system error, "Render Cache Loading Data.xsl" after selecting certain forms in the System Administration Tool navigation pane.	Internet Explorer dll responsible for rendering XML (msxml3.dll) not properly registered.	Re-register the dll as follows: 1. From Windows Start menu select Run. 2. Type 'regsvr32 msxml3.dll' 3. Click OK on the dialog box.
		Page 4 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
System Administration Tool Online help is not available. When you click on the help buttons in the System Administration Tool, the help window displays “404 Page Not Found” error.	Online help files are not installed either locally on the 3300 ICP system or remotely on a web server.	Install online help locally on your PC or remotely on a web server **Locally**: 1. Copy the /Documentation/Help.zip file from the 3300 ICP software CD-ROM to the hard drive on your PC. 2. Using WinZip, extract the files to a folder on your PC. 3. Open the “sy sad min” folder and locate the “sysadmin.html” file. 4. Create a shortcut on your Desktop to the “sysadmin.html” file. 5. Double-click the “sysadmin.html” shortcut to launch the help. 6. Navigate to the required help topic by using the Table of Contents, Index, or Search field. Remotely: 1. Copy the /Documentation/Help.zip file from the 3300 ICP software CD-ROM to the web server. 2. Using WinZip, extract the files to a folder on the web server. 3. In the Remote Help Server field of the System Options form, enter the enter the URL to the location of the help files using the following syntax: http://<IP Address of Remote Server>/help/ For example: http://10.117.7.39/help/ where 10.117.1.39 is the IP Address of the remote help server. 4. Click Save.
	URL to the remote help files is entered incorrectly	Enter the correct URL to the help files on the web server. You enter the URL to the help in the Remote Help Server field of the System Options form.
		Page 5 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
You receive a Runtime error when you attempt to access the Mitel Customer Documentation site (edocs.mitel.com) from the 3300 ICP System Administration Tool Online Help	If script debugging is enabled in Internet Explorer, you may get a runtime error when accessing the Mitel documentation web site from the MCD System Administration Tool Online Help.	This does not prevent the web site from opening. Close the error window to access the website.To prevent this runtime error from appearing, disable script debugging in Internet Explorer: 1. In the Internet Explorer Tools menu, select **Internet Options**. 2. In the Advanced tab, select the **Disable Script Debugging** check box. 3. Click **OK**.
The Export button in a System Administration tool form fails to launch the Microsoft Excel spreadsheet,	Pop-up blocker is enabled, preventing Excel Spreadsheet from opening.	Disable the pop-up blocker in your browser. 1. In Windows Explorer, click Tools > Folder Options. 2. Click the File Types tab. 3. In the Registered File Types list, select the XLS Microsoft Excel Worksheet type. 4. Click the Advanced button. 5. Clear the Browse in same window box. 6. Check the Confirm open after download box. 7. Click OK, and then click Close.
Importing form data fails to start on PC with Windows 7, Vista, Windows XP and Internet Explorer 9.0.	Wrong version of Java plugin installed. You must have the version (32-bit or 64-bit) that matches the version of IE 9 installed. The default version installed with Windows is 32-bit.	Verify if you are using 32-bit or 64-bit browser Internet Explorer: 1. Launch Internet Explorer. 2. Click on the Help menu at the top. 3. Select About Internet Explorer which will bring up an information window. If version of IE displays 64-bit Edition, then it is 64-bit IE, otherwise it is a 32-bit browser. Go to the Java website (http://java.com/en/download/) and download the required version.
Data errors occur when you use the Import Spreadsheet to import data into the System Administration Tool.	CSV files generated by the Import Spreadsheet and subsequently modified using Microsoft Excel may cause errors after you import them into the 3300 ICP.	Use Windows Notepad or other text editor to edit the file or edit the original worksheet in the Import Spreadsheet and regenerate the. Comma Separated Values. A type of database file that separates data fields with a comma.*csv* file.
		Page 6 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
Unable to complete a Form Print and or complete a Logs Capture from the System Diagnostics Reporting form of the System Administration Tool	System Name is unknown. Check the top left corner of the System Administration Tool main window to verify that the system name is programmed properly.	If the System Name is unknown, enter a System Name in the Network Elements form.
System export of logs fails with error when running Windows XP with SP2	Internet Explorer settings	1. Open Internet Explorer. 2. On the **Tools** menu, click **Internet Options**. 3. On the **Security** tab, click **Custom Level**. 4. Do one or both of the following: • To turn off the Information Bar for file downloads, in the **Downloads** section of the list, under **Automatic prompting for file downloads**, click **Enable**. • To turn off the Information Bar for ActiveX controls, in the **ActiveX controls and plug-ins** section of the list, under **Automatic prompting for ActiveX controls**, click **Enable**. **Note:** Windows XP with Service Pack 2 (SP2) provides a higher level of security than previous versions. It is possible that this increased security may affect the way the 3300 ICP works. If you need to maintain this level of security, see your System Administrator.
MCD Software Installer Tool		
MCD Software Installer fails with “Failing to Read from LOS”	Two NICs installed on the PC and trying to connect to a pre-3300 Rel 7.0 switch	1. Disable the wireless NIC. 2. Reboot PC.
The online upgrade procedures fails, and the MCD Software Installer tool presents the following error message “The username provided couldn't log in”.	Controller has a System Type of “Standalone” and is therefore not licensed for IP Networking or XNET.	Choose **Offline Upgrade** or do full install.
MCD Software Installer tool displays “Unable to retrieve specified file” error when executing step 1 of the tool.	The MCD Software Installer tool looks for a file entitled _swrevs in the FTP Server's default local path folder. The tool will not proceed to step 2 without this file being present.	Refer to Mitel Knowledge Base article 07-4409-00026
		Page 7 of 9

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
Unable to turn off Windows XP Firewall before using the MCD Software Installer	You don't have administrative privileges on the PC running the MCD Software Installer tool. This will cause a problem when you attempt to turn off Windows XP Firewall which is on by default in Windows XP SP2. In this case, if you select the PC running the SI tool as the FTP source for the 3300 ICP installation files, the file transfer will be blocked by the Windows XP SP2 firewall.	Go into the PC services, and stop the Following Service (Windows Firewall / Internet Connection Sharing ICS). This should disable the Windows Firewall Service all together. Another option is to select the 3300 as the FTP server (you can configure this option in the newer versions of the SI tool). However, if you have to do manual software install then you have no option but to manually stop the Windows Firewall Service in the Installer PC which will require local administrator rights to the PC.
Desktop User Tool		
The Desktop Tool displays a license violation message when you log in or out.	The controller is in license violation mode.	Correct the license violation event.
The Desktop Tool is disabled.	An over-allocation license violation event has been left uncorrected.	Correct the license violation event. In this case, you must reduce or eliminate the number of over-allocated licenses.
With Windows XP Service Pack 2, a user profile with Desktop Administration access is unable to log in. The user experiences the following symptoms: • When the user enters the Login ID and Password and clicks OK, nothing happens, and • user is returned to the login page.	Pop-up blocker feature	Disable the pop-up blocker feature in the browser Internet Options. To disable pop-up blocker: 1. Open Internet Explorer. 2. Click **Tools > Internet Options**. 3. On the Privacy tab, clear the "Block pop-ups" check box. Refer to Mitel Knowledge Base article 05-5157-00001
Audio File Download (for Music on Hold and Greetings)		
Audio File cannot be located	Corrupted file	Verify that the audio file is not corrupted.
Audio File is rejected	Incorrect audio file specifications	Verify that the audio file meets the required specifications (see System Audio File Update form in the System Administration Tool).
System Greeting is in the wrong language	Incorrect language file downloaded	Download a file in the correct language using the System Audio File Update form or Enterprise Manager.
System error log is generated	Downloading file when system is unavailable	Verify that you are not downloading a file during a backup, restore or upgrade, or while someone is recording the same greeting from a telephone.

Table 39: System Administration Tool Troubleshooting

Symptom	Probable Cause	Corrective Action
Unable to complete a Form Print and or complete a Logs Capture from the System Diagnostics Reporting form.	System Name is unknown. If the System Name is programmed properly, it appears in the left corner of the System Administration Tool window.	Enter the System Name properly in the Network Elements form.
ISDN Maintenance & Administration Tool (IMAT)		
Receive a “missing DLL file” error while loading IMAT software on PC running Windows 98.	Missing required DLL file.	Obtain and install required DLL file. Refer to Mitel Knowledge Base article 05-3849-01044. The required DLL file is attached to this article.
When you use IMAT to retrieve the database from the Universal NSU, the database files do not appear to have been downloaded	NSU is running as ISDN node.	Refer to Mitel Knowledge Base article 06-5104-00038.
		Page 9 of 9

Automatic Call Distribution

Table 40: ACD Troubleshooting

Symptom	Probable Cause	Corrective Action
Calls stay in Queue and are not rerouted to path unavailable point.	Programming error.	Refer to Mitel Knowledge Base article 06-5163-00009
ACD RAD ports don’t play for incoming calls on SIP Trunks	Programming error.	In the SIP peer profile, make sure that “Suppress Use of SDP Inactive Media Streams” is set to NO. Refer to Mitel Knowledge Base article 07-5157-00018 for more information.
The “Generic Group Alert” key does not work.	The Generic Group Alert function is intended to display single queue status when an agent logs in. If the agent belongs to multiple groups, the function does not know which group to display and will not work.	To display the queue status for each group that includes that particular agent, program a “Specific Group Alert” key for each group.

Hot Desking

Table 41: Hot Desk Troubleshooting

Symptom	Probable Cause	Corrective Action
When a hot desk user attempts to log in, the following error message appears on the display of the IP phone: “Error: feature failure”. Both the hot desk enabled set and the hot desk user are local on the 3300 ICP.	The PBX Number and the Cluster Element ID that are programmed for the 3300 ICP do not match.	Ensure that the PBX Number in the ICP/PBX Networking form matches the Cluster Element ID in the Cluster Elements form.
“Phantom” ringing occurs when an ACD Hot Desk Agent is logged into an ACD.	The user profile for a hot desk agent supports up to 47 programmable keys. If an agent is assigned 47 feature keys and then logs into an ACD hot desk set that has fewer than 47 programmable keys on it, the extra keys are not accessible. If one of these “inaccessible” keys is programmed as a line appearance, calls for the line appearance will still ring at the phone.	To avoid this problem, choose one device type that supports 13 programmable keys, program a consistent layout for the buttons, and provide printed button templates for each ACD hot desk set.

Emergency Call (E911) Support

Table 42: Emergency Call Support Troubleshooting

Symptom	Probable Cause	Corrective Action
Emergency calls do not trigger E911 local notification. Calls placed on a designated “emergency” route do not trigger local notification.	E911 local notification will not be activated *if an emergency hunt group is not fully programmed and a is* call placed on a designated “emergency” route.	Refer to Mitel Knowledge Base article 04-1000-00020 for programming instructions.

Table 42: Emergency Call Support Troubleshooting

Symptom	Probable Cause	Corrective Action
Emergency call does not trigger E911 local notification	Enhanced 911 (E911) operation not fully supported for the device. There are some exception cases whereby emergency calls do not trigger E911 local notification.	None. Currently, the following devices do not fully support Enhanced 911 (E911) operation: • Hot Desk users • IP consoles • Teleworker Solution users • Your Assistant and Your Assistant Softphone users • Any other mobile IP phones or phones that are carried from location to location. Refer to the Engineering Guidelines for details.

Embedded Voice Mail

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
After upgrading from 8.0 to MCD 4.0 UR4 (10.0.4.14) the embedded voice mail fails to start. Monitoring the RTC you will see the following: Starting iPVM Version 9.2.1.4 *** Fatal error starting the voice driver. iPVM stopped. Voice Mail Did not start Successfully	Obsolete DSP (Quad DSP 21061) installed.	Replace with a Quad 21161 or DSP II depending on the platform and function they are being used for.
Notification calls are configured for a mailbox but don't seem to work.	Notification is not enabled at the system level.	Enable notification in VM Options form.
	CO line access is restricted for voice mail port extension numbers.	Ensure that voice mail port numbers are not restricted from access to CO lines.
Notification calls use the correct outside lines but the pager never beeps.	Notification phone number or pager type programmed incorrectly.	Check the notification phone number and pager type.
		Page 1 of 7

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
The date and time that a message was left is incorrect.	3300 ICP system clock is wrong.	Adjust 3300 system date and time using the WriteDateTime maintenance command.
The system is warning that the disk space is almost full.	Too many voice mail messages stored in mailboxes.	Delete unused mailboxes and have subscribers clean out unnecessary saved messages.
Too much silence before or after a greeting or mailbox name.	Hesitating before starting to record. Waiting too long before ending recording.	When recording greetings and names, start speaking immediately after the tone and press any key as soon as you are finished.
When outside callers reach the auto attendant and press 0, either no phones ring or the incorrect phone rings.	Mailbox 0 is not associated with operator’s extension.	Check that mailbox 0 is correctly associated with the operator's extension.
When outside callers reach the auto attendant press 0, the operator's telephone rings and never forwards to voice mail.	Call Forwarding not set correctly on the Operator’s phone.	Set Call Forward-Busy/No Answer on the Operator's phone to forward to voice mail.
Internal/external callers occasionally reach the Operator when calling the auto attendant.	The voice mail ports are all busy.	Try again later.
Message Waiting indication is slow to appear	Not enough voice mail ports.	Ensure that all 20 voice mail ports in the VM Ports form are programmed.
MWI light is flashing in the morning but no new messages waiting (i.e., phantom MWI).	Obtain the System Diagnostic Logs (see "System Diagnostics Reporting" in ESM Help). Untar the logs file and open the diag.dat file in Notepad. Search for 3 a.m. Look for the MWI On code and mark down all extensions or numbers that the MWI is being set on. You may find a system speed dial or hunt group number that has an association to the extension that is complaining about the phantom MWI. This could mean you have a voice mail box associated with the system speed dial that points to the extension, or a hunt group that has the DN as its first member.	Change programming.
		Page 2 of 7

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
The greeting is played twice.	The bilingual option is enabled in the VM Prompt Languages form and the second language is set to the same greeting as the first language.	Disable the bilingual option in the VM Prompt Languages form, or record or download a bilingual greeting.
The voice mail system is not responding after all 20 ports are programmed.	Voice mail application is not initialized on ports.	Restart the 3300 ICP system using the Reset System maintenance command to initialize the voice mail application on all ports.
The voice mail system resets itself at times.	In the event of a critical error, the voice mail system resets.	Contact Mitel Technical Support.
A minor alarm is raised after adding voice mail ports.	Not enough DSP resources available in the system.	Add more DSP resources. To calculate the amount of DSP resources that will be required for your system, please see the 3300 Engineering Guidelines.
Callers are greeted by a FAX tone instead of the company greeting.	Programming error.	See “System Greetings” and/or “RAD Greetings” in the System Administration Tool online help for programming instructions.
Cannot modify voice mailbox settings from the Group Administration Tool.	Voice mailbox length and directory number length are different.	If the voice mailbox length and directory number length are different, you can only edit voice mailboxes from the System Administration Tool or the system Administrator Mailbox.
Callers are transferred to Auto Attendant when pressing a Personal Contact key.	An invalid phone number was programmed.	Reprogram the Personal Contact.
	The account code length is the not the same as the mailbox length.	In the Class of Service Options form, set the account code length to the same value as the mailbox length.
An IP Integrated voice mail Auto-Attendant (for example NuPoint IP, 6500 S@E, 6510 UM) fails to transfer a call to an extension.	The name in the Telephone Directory starts with tilde (~) character. The application will dial the extension but the transfer can not be completed if the name starts with a tilde character.	Delete the tilde (~) character from the name in the Telephone Directory form.
When an external trunk is speed-dialed to the embedded Auto Attendant, the incoming caller receives the wrong greeting of “Please Enter a Mail Box number”. The Auto Attendant greeting should be heard instead.	Improper options are enabled in the Auto Attendant's Class of Service.	Set the following COS options to either both “Yes” or both “No”. • “Display ANI/DNIS/ISDN Calling/Called Number” • “Display ANI/ISDN Calling Number Only”
		Page 3 of 7

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
Users suddenly cannot access Visual Voice Mail.	Range programming in progress.	While an administrator is using range programming in the System Administration Tool to modify the system database, users will be unable to access Visual Voice Mail. Perform range programming outside of regular business hours.
Voice mail has choppy audio and words are missing from the greetings and messages.	Management Access Point (MAP) connected directly to a 3300 ICP 10/100 Base T ethernet port.	Do not connect the Management Access Point (MAP) or any other devices directly to the 3300 ICP 10/100 Base T ethernet ports. The Management Access Point uses 10 Mbps half duplex which causes a high collision rate on the Ethernet port resulting in poor audio quality. Only connect other Layer 2 switches to the 3300 ICP Ethernet ports.
Unable to add or edit mailboxes. Attempts result in an error message, “A Voice Mail Server Name for a local mailbox must match System Name.”	Voice mail server host name doesn’t match 3300 ICP system name.	The host name of the voice mail server in the VM Network Servers form must match the entry in the Name field in the Network Elements form. To correct the problem, change the Name field in the Network Elements form to match the voice mail server name.
Embedded Voice Mail cannot transfer or page externally (fails or rings only once).	Supervised Transfer is enabled, and the Transfer Ringback Timeout is too short.	In the VM Options form, disable the “Enable Supervised Transfer” or increase the “Transfer Ringback Timeout.” The default is 4 seconds and that is not long enough to accommodate external transfers.
Embedded RAD does not answer.	If a incoming call is blind-transferred to an Embedded RAD, the embedded RAD will experience “ring no answer” and/or “Do Not Disturb” conditions.	1. Ensure that the embedded RAD port is in a RAD Hunt group. 2. Program the phase timer of RAD hunt group to be 1 second or higher 3. Ensure that all calls are transferred to the RAD Hunt group. Call should not be made directly to the RAD port.
When voice mail is forwarded to e-mail, the e-mail indicates an incorrect sent time.	The wrong time being shown in e-maills forwarded from voice mail usually indicates that the Time Zone is not set correctly. The default value is GMT - 4:00.	In the VM Network Servers form of the System Administration Tool, change the Time Zone field to match your time zone.
		Page 4 of 7

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
Voice mail integration fails between an SX-2000 and a 3300 ICP that is acting as a voice mail server.	Integration fails if all of the following conditions are present: • Systems are connected through a MSDN link • COS for the voice mail MSDN link has **COV/ONS/E&M voice mail port** option enabled. • Diversion is turned off on both systems.	• Disable the **COV/ONS/E&M Voice Mail Port** option, or • Enable Diversion on both the 3300 ICP and the SX-2000.
Users cannot program Forward to E-Mail using the Desktop Tool.	Programming incomplete.	1. Verify that the Advanced Forwarding purchasable option is enabled in the License and Options Selection form. 2. Verify that Forward to E-mail is enabled for that user (see Forward to E-mail feature description in the System Administration Tool online help). 3. Ensure feature is programmed on the user's set. If you have a centralized Networked Voice Mail voice mail server configuration, users can only program Forward to E-mail using the telephone interface.
User needs to recover a voice mail message that he or she has forwarded; however, "Delete After Forwarding" is enabled.	If Delete After Forwarding" is enabled, voice mail messages are deleted from the user's mailbox as soon as the message is forwarded.	All sent messages are available for a limited time in the /vmail/vpim/sent folder (see Networked Voice Mail Detailed Description). Administrators can recover them from this folder using FTP, and then e-mail the recovered message to the user. **Note:** Users will need an audio editing tool to listen to the recovered message. Standard media players (such as those from Microsoft) cannot play Mitel voice mail messages directly. **Note:** Once the message is deleted from the /vmail/vpim/sent folder, the message is irretrievable.
ALL Visual Voice Mail users get the following response when they try to access a message. "NO AUDIO CONNECTION"	Mitai/MitaiServerAddressForLocalApps field in the Controller Registry Configuration Form is programmed with an external IP address.	Ensure that the Mitai/MitaiServerAddressForLocalApps field in the Controller Registry form is not programmed with an external IP address. The default for this IP address is 0.0.0.0. Reset the IP address for this field to 0.0.0.0, and then reboot the system to effect the change.
		Page 5 of 7

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
Telephone only rings once OR Call transfer fails.	Supervised transfer timed out.	In the ESM VM Options form, disable the “Supervised Transfer” option OR increase the “Transfer Ringback Timeout” (the default is 4 seconds)
Minor Alarm is raised.	Not enough DSP Resources available.	Add DSP resources. See “Increasing DSP Resources” in the “Installation Planner” chapter of the *MCD Technician’s Handbook.*
Sent time is wrong on e-mails forwarded from voice mail.	Time Zone not set correctly in Voice Mail programming.	In the ESM VM Network Servers form, program the “Time Zone” field.
Voice mail audio is choppy and words are missing from greetings and messages.	The 7100 Management Access Point (MAP) or other device is connected directly to the 10/100 BaseT Ethernet ports.	Only other Layer 2 switches should be connected to the Ethernet ports.
	The 7100 Comms port is connected directly to the Maintenance port.	The 7100 Comms port on the 7100 MAP must only be used for programming the MAP unit. Once the MAP unit has been programmed, the maintenance port on the 3300 must be connected using serial interface 1 (port 1) or serial interface 2 (port 2) on the MAP 7100.
Message waiting lamp is on but there is no message in your mailbox.	Multiple possible causes.	Refer to Mitel Knowledge Base article 05-5107-00006 for a list of possible causes and corrective actions.
	The default mailbox of the 3300 ICP is mailbox zero. If the user has a line appearance key of directory number zero programmed, then any messages in the default mailbox cause the MWI on the extension to be lit.	Change the default mailbox number of the 3300 ICP.
MWI lamp on ONS sets failing to light.	Message Waiting Lamp disabled in circuit descriptor and/or ONS CLASS/CLIP Message Waiting option incorrectly set.	Verify that the circuit is assigned an ONS/OPS Circuit Descriptor that has the Message Waiting Lamp field on set to “Yes.” Verify that CLASS/CLIP sets have a COS with the ONS CLASS/CLIP Message Waiting option set to “Yes” and that non-CLASS/CLIP sets have a CoS with the same option set to “No.”
		Page 6 of 7

Table 43: Embedded Voice Mail

Symptom	Probable Cause	Corrective Action
In the VM Mailboxes form of the System Administration Tool, voice mail boxes appear multiple times, or groups of voice mail boxes may repeat when changing from page to page.	Possible voice mail database corruption.	Refer to Mitel Knowledge Base article 07-4409-00023.
Embedded RAD does not answer (ring no answer) or returns Do NOT Disturb (DND) tone.	If an incoming call is blind-transferred to an Embedded RAD, the embedded RAD will experience “ring no answer” and/or “Do Not Disturb” condition.	1. Ensure that the embedded RAD port is in a RAD Hunt group. 2. Program the phase timer of RAD hunt group to be 1s or higher. 3. Ensure that all calls are transferred to the RAD Hunt group and that no one calls directly to RAD port.
Embedded voice mail fails to page external, or fail to perform supervised transfer to external number.	Programming conflict.	Refer to Mitel Knowledge Base article 06-5191-00068.
Embedded voice mail goes out of service after “Load Controllers” command issued	The “Load Controllers” command is used to reboot the Peripheral Cabinet and/or the DSU. This has had the unexpected effect of causing the Embedded Voice to go out of service.	Avoid the use of the “Load Controllers” command. To do this you must physically reset the Peripheral Cabinet and/or the DSU. If this command has already been issued reset the 3300 controller to get the embedded voice mail back in service.
Voice mail message playback contains noise or audio level is too low.	Incorrect Balanced Network Setting or Trunk Category in the Trunk Circuit Descriptor form of the LS trunk that the message came in on.	Use the Line Quality Measurement form in the System Administration Tool to determine the correct settings.
User receives extra audio (tones and noise) on his or her voice mail message	Voice Mail system is not starting or stopping the recording at the right time due to incorrect correct tone detection file.	In the License and Option Selection form, ensure that the Country field is set correctly for the system. The Country setting determines the default language, dialing plan, tone plan, and loss and level plan for the system. Refer to the Hardware Technical Reference Manual for tables that list the Tone Plans.
		Page 7 of 7

Networked Voice Mail

Table 44: Troubleshooting Networked Voice Mail

Symptom	Corrective Action
Internal system error when adding voice mail boxes.	Ensure that the name of the networked voice mail server matches the system name of controller.
A mailbox number is not recognized when creating or forwarding a voice message.	1. Make sure that the Networked Voice Mail option is enabled on all nodes. 2. Make sure that the Primary Node ID length is the same for all nodes. 3. Make sure that all mailboxes (excluding resiliency mailboxes) have different numbers. 4. Make sure that the mailbox length is the same for all nodes.
A mailbox number is not recognized when creating or forwarding a voice message to a remote mailbox on another cluster.	Enter the PNI before the mailbox number when addressing a message to a remote mailbox.
The voice messages for resilient users are received in their mailboxes on the secondary controller while the user devices are on the primary controller.	If a caller leaves the resilient user a voice message while the user's device is on the secondary controller, the message is recorded in the user's mailbox on the secondary controller. However if voice messages are being recorded in the mailbox on the secondary when the user's device is on the primary, ensure that the voice mail server is configured correctly. In a distributed voice mail configuration, ensure that the user's voice mail server is on their extension's primary controller.
Message sent to a known valid user is returned with Failed to Deliver message.	1. Ensure that the remote server is available. 2. Ensure that the remote server has not failed over to its secondary server. 3. Ensure remote node is programmed properly in the VM Network Servers form. 4. If you have a centralized voice mail configuration, make sure that the user's voice mail server is not configured on the primary ICP of the user’s extension.
User can't use Dial-by-Name feature.	Dial-by-Name is not available for remote mailboxes.
Voice mail has choppy audio and words are missing from the greetings and messages.	The Management Access Point (MAP) is connected to 3300 ICP 10/100 Base T ethernet ports. Do not connect the Management Access Point (MAP) or any other devices directly to the 3300 ICP. The Management Access Point uses 10 Mbps half duplex which causes a high collision rate on the ethernet port resulting in poor audio quality. Only connect other layer 2 switches to the 3300 ICP ethernet ports.
	Page 1 of 2

Table 44: Troubleshooting Networked Voice Mail

Symptom	Corrective Action
You see the following log while you are monitoring the RTC shell on boot up: Starting up VM Corp Dir... ...Fault detected while starting up VM Corp Dir. Starting up SMTP Client Starting up SMTP Server tAppStartup ProcessorCoordinator started component ADAPTATION_LAYER_COORDINATOR tAppStartup ProcessorCoordinator started component APPLICATION_LAYER_COORDINATOR ResourceAlarmStartup ready. Task StartupHwRst being deleted while ACTIVE Voice Mail Starting in 0 minutes. Starting iPVM Version 6.21.00 Voice Mail Successfully Started.	This log appears if you haven't enabled Networked Voice mail in the license. If you see “Voice Mail Successfully Started” at the end of this log, you will be able to log into the System Administration tool and your phones will come up.
Voice messages are not compressed.	None. Networked Voice Mail does not support compression.
	Page 2 of 2

Station Message Detail Recording

Table 45: Station Message Detail Recording Troubleshooting

Symptom	Probable Cause	Corrective Action
IP trunk call unsupervised transfer and queued to ACD path reports path extension instead of path reporting number.	Refer to Mitel Knowledge Base article 06-9999-00002 for possible causes.	Refer to Mitel Knowledge Base article 06-9999-00002.
When making a call in or out on SIP trunks the trunk number in the SMDR record is blank.	SMDR for SIP Trunks use the SMDR Tag field from the SIP Peer Profile form for the trunk number. If this field is blank, the trunk number in the SMDR record is blank.	Enter a Trunk Number (for example, 99) in this field and the number will be displayed as the trunk number in the SMDR record (for example, T099).
Entering a non-verified account code during a call generates a single SMDR record instead of the normal two, one for the initial call and a second for the subsequent account code entry.	Account code entered within five seconds of call answer.	Change the "Suppress Initial SMDR record with Account Code Entered Time" in the SMDR Options form in ESM. The default is five seconds which generates one SMDR record if the account code is entered within 5 seconds of answering a call. If the account is entered after 5 seconds, two records are generated.

Unified IP Client for Sun Ray

Table 46: Unified IP Client for Sun Ray Troubleshooting

Symptom	Probable Cause	Corrective Action
Solaris X server fails to provide graphical display on the console port. After you instal UIPC version 1.0 UR1, the following error is displayed on the SunRay Server console after a Sun Server reboot: ********** See File/var/dt/Xerrors for details ********** - bash - 3.00# - bash - 3.00# ********** The X-server can not be started on display: 0 . . . . See File/var/dt/Xerrors for details **********	Error in XF86Config file.	Refer to Mitel Knowledge Base article 09-5160-00009.

CHAPTER 8

VOICE NETWORKING

Voice Networking Troubleshooting Tips

- ☑ Refer to the Voice Networking book in the System Administration Tool online help for information on Voice Networking.
- ☑ To view and manage pending (in-progress) SDS distribution updates and update errors, see the SDS Distribution Errors form in the System Administration Tool online help.

Bandwidth Management

Table 47: Troubleshooting Bandwidth Management

Symptom	Possible Cause	Corrective Action
Bandwidth Statistics show duplicate CAC rejections.	ARS Routes not programmed correctly.	Ensure that ARS Routes form is programmed correctly.
Bandwidth Statistics are not being generated at the ZAPs.	Bandwidth Statistics and Reporting is not enabled.	Enable Bandwidth Management Statistics and Reporting in the Bandwidth Management Configuration form.

Clustering

Table 48: Troubleshooting Clustering

Symptom	Possible Cause	Corrective Action
Unable to place calls between systems via IP trunks in a clustered, redirected, or resilient environment.	PBX Number in the ICP/PBX Assignment forms of the systems are programmed incorrectly.	For each system in the cluster, ensure that the system's PBX Number matches its CEID Index Number as defined in the Cluster Elements form.

IP Networking

See "IP Trunking (IP Networking)" on page 129.

Multi-Node Management

MNM Fault Management

Table 49: Troubleshooting MNM Fault Management

Symptom	Possible Cause	Corrective Action
MNM Fault Management not functioning.	Too many elements in MNM Administrative Group.	MNM applications are only supported for up to 20 elements in an Administrative group. After you add the 21th element to the group, the MNM applications are disabled for the entire group. Reduce the number of elements to 20 or fewer.
	MNM Fault Management has been disabled.	Enable Fault Management in the Admin Group Fault Management form.
Alarm status on remote elements not accurately reflected in Admin Group Alarm Summary form. For example, form shows alarms on remote elements when there are no alarms present.	SNMP Configuration form is improperly configured on Admin Group member elements. Note: Alarm status changes on member elements take several minutes (typically 5 to 10) to register in the Admin Group Alarm Summary form.	Provision the SNMP Configuration form on all Admin Group members as follows: 1. Set "Enable SNMP Agent" to "Yes." 2. Configure the Community strings. 3. Set "Accept Requests from All Managers" to "Yes" or leave it at "No" and enter the IP addresses of the Admin Group elements you want to accept SNMP messages (including alarms) from. For more information, see Multi-Node Fault Management in the System Administration Tool Help.

MNM Backup and Restore

Table 50: Troubleshooting MNM Backup and Restore

Symptom	Possible Cause	Corrective Action
MNM Backup and Restore not functioning.	Too many elements in MNM Administrative Group.	MNM applications are only supported for up to 20 elements in an Administrative group. After you add the 21th element to the group, the MNM applications are disabled for the entire group. Reduce the number of elements to 20 or fewer.
	FTP server is down.	Ensure FTP server is working properly and that there is sufficient disk space on the server for the database files.
	Not enough client sessions available on FTP server.	Ensure that the FTP server supports the required number of concurrent client sessions. For example, if the Administrative Group has 10 elements, the FTP server must support a minimum of 10 concurrent client sessions.

MNM Application Reach Through

Table 51: Troubleshooting MNM Application Reach-Through

Symptom	Possible Cause	Corrective Action
Cannot reach through to an element in the Administration Group.	Element has pre-MCD Release 4.0 software installed.	Upgrade element to MCD Release 4.0 or later software.
	Form incompatibility. The requested form is not supported. The local element has a later software version than the remote element and the selected form does not exist in the software version on the remote element.	Upgrade elements to same software version.
	Form not licensed. Some forms, such as the Fax Service Profiles form must be licensed on the element before they are available. If a form is licensed on the local element, but not licensed on the remote element, you cannot modify it.	License the functionality associated with the form on the remote node.

Page 1 of 2

Table 51: Troubleshooting MNM Application Reach-Through

Symptom	Possible Cause	Corrective Action
Application Reach-Through request fails.	User authorization profile is out of sync on the remote node	Use SDS to sync the User Authorization Profiles form across the Administrative Group.
	A network problem is preventing the local element from connecting to the remote element.	Contact your IT Support administrator.
	You do not have permission to access the requested form on the remote element. The Admin Policies form is not synchronized across all the elements in the Administrative Group.	Ensure that SDS is sharing the Admin Policies form to all elements in the Administrative Group.
Cannot find user on remote element.	User does not exist on the remote element because the user information was not distributed to the remote element by SDS.	Resolve any SDS pending updates or errors on the local element. Refer to the System Administration Tool online help for instructions.
After you select a remote element in the **Show form on** field and click **Go**, Internet Explorer does not open the form of the remote element.	IP address of the remote Administrative Group element has not been added to the Local Internet zone of the Internet Explorer browser on your client PC.	Add the IP addresses of the remote elements to the Local Internet Zone of your PC. • Click your Internet Explorer browser. • Click **Tools**, and then click **Internet Options.** • Click the **Security** tab, and then click **Local Intranet**. • Click the **Sites** button. • Click **Advanced**. Leave all boxes in this dialog box checked. • Enter the IP addresses of the Administrative Group elements. • Click **Add**. • Click **Close**, and then click **OK**.
Remote element not listed in **Show form on** field in Mozilla Firefox	Remote element running incompatible MCD software.	Upgrade remote element to MCD Release 6.0 SP1 (or later) or switch to Internet Explorer 8.0 (or later).
		Page 2 of 2

Resiliency

IP Device Resiliency

Table 52: Troubleshooting IP Device Resiliency

Symptom	Possible Cause	Corrective Action
All resilient devices are not functioning (no dial tone) after the primary ICP goes out of service.	Secondary ICP is not in service.	Ensure that the secondary ICP is operating.
	IP phones are not provisioned as resilient.	Enter the Locate commands on the secondary ICP to determine the status of the IP phone. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone. If not, provision the IP phones for resiliency, using the System Administration Tool. Refer to the System Administration Tool Online help.
	Cluster is not programmed correctly.	Enter the Locate commands (see "Locating Resilient Devices" on page 217) on the secondary controller to determine the status of the IP Phone. Refer to *Voice Networking -> Configure Network* in the *System Administration Tool Online Help* for procedures on the following tasks: 1. Ensure that the optional software required for clustering is enabled at each element. 2. Ensure that each resilient IP device is connected to a controller that has Release 4.0 or later. 3. Ensure that each element in the cluster is assigned a unique CEID in its Cluster Elements form. 4. Ensure that ARS is programmed correctly to route calls to all the other elements in the cluster. 5. In the Cluster Elements form ensure that you have programmed the Feature DN fields. 6. In the ICP/PBX Networking form of each element, ensure that the PBX Number matches the CEID index number that is programmed in the Cluster Elements form. 7. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone.
		Page 1 of 6

Table 52: Troubleshooting IP Device Resiliency (continued)

Symptom	Possible Cause	Corrective Action
Resilient phones do not fail over to their secondary ICP when their primary fails.	The network may not be clustered or it may have been improperly clustered.	To learn how to properly cluster a network, go to http://edocs.mitel.com, and refer to *Voice Networking -> Configure Network* in the *System Administration Tool Online Help*. If you have clustered your network, verify that it has been properly clustered. Using the System Administration Tool on each 3300 ICP, verify that the Cluster Element Index in the Cluster Elements form has the same value as the PBX Number in the ICP/PBX Networking form. (In the Remote Directory Numbers form, look up the number of the phone or phones that are not failing over. Note the CEID number for the phones. Check the CEID numbers against those for the phones in the ICP/PBX Networking form. The numbers must match, and their values must not be higher than 256.
		On each phone that is not failing over, use the debug function to verify that its current ICP list contains a primary and a secondary ICP. On a 5140/5240 IP Appliance 1. Hold down both volume keys at the same time, and dial **33284** (“debug”) to display debug options. 2. Press **Network**, and then press **ICP Server IP(s)**. Another set of options are displayed. 3. Check the options, starting at the bottom of the list: - Press PBX Connection Info. The appliance should display “PBX Connection Status TCP Link Active”, which indicates that the appliance is in service and communicating with its primary ICP. - Press **Current ICP Server** to display the current ICP address that the appliance is communicating with. - Press **Current ICP Index**. The appliance should display “Current Server Index is:1, List Length is: 2" to confirm that the appliance has a list of 2 ICPs. - Press **IP Server Address 1** to display the IP address of the primary ICP. - Press **IP Server Address 2** to display the IP address of the secondary ICP. If the appliance is resilient, it displays an IP address for its secondary ICP. Verify that this IP address is correct. If the phone does not display an IP address for a secondary ICP, use the **User and Device Configuration** form in the System Administration Tool to provision the device with a secondary ICP.
		Page 2 of 6

Table 52: Troubleshooting IP Device Resiliency (continued)

Symptom	Possible Cause	Corrective Action
Resilient phones do not fail over to their secondary ICP when their primary fails.	The network may not be clustered or it may have been improperly clustered.	On a 5020/5010 IP Phone 1. Hold down both volume keys at the same time, and dial **33284** ("debug") to display debug options. 2. Press **Superkey** until **Network** is displayed. 3. Press the **volume-down** key until **Network – PBX IP <IP address>** is displayed. This is the address of the phone's current ICP. 4. Press either the volume-up or volume-down key until **Network – PBX IP <address> #1** is displayed. This is the IP address of the phone's primary ICP. 5. Toggle the volume keys (press the volume-down and then the volume-up key, or vice versa) to display **Network – PBX IP <IP address> #2**. This is the IP address of the phone's secondary ICP. Verify that this IP address is correct. If the phone does not display an IP address for a secondary ICP, use the User and Device Configuration form in the System Administration Tool to provision the device with a secondary ICP.
One or more resilient phones are not functioning (no dial tone) after the primary ICP goes out of service	An IP device license is not available for the affected device(s) on the secondary ICP.	Ensure that you have provisioned enough IP device licenses on the secondary ICP. Refer to the *MCD Resiliency Guidelines* for details.
	May indicate a network failure.	Verify the network.
One resilient phone is not functioning (no dial tone) after its primary ICP goes out of service.	IP phone is not provisioned as resilient.	Enter the Locate commands (see "Locating Resilient Devices" on page 217) on the secondary ICP to determine the status of the IP phone. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone. If not, provision the IP phones for resiliency, using the System Administration Tool. Refer to the System Administration Tool Online help.
While on a call at a resilient phone, the primary ICP goes out of service and the call is immediately dropped (no call survival). After you hang up the IP phone and go off-hook again, the IP phone is functioning on its secondary ICP.	The call was connected through a TDM trunk (for example PRI trunk) on the primary ICP that failed.	Program IP trunking on all ICPs.
		Page 3 of 6

Table 52: Troubleshooting IP Device Resiliency (continued)

Symptom	Possible Cause	Corrective Action
While on a call at a resilient phone, the primary ICP goes out of service, and the call is immediately dropped (no call survival). After you hang up the IP phone and go off-hook again, the IP phone remains out of service.	Network failure (for example a Layer 2 switch that connects the IP phone to both the primary and secondary ICPs goes down).	Program redundancy into the network layer.
After an IP phone fails over to its secondary ICP, you can make calls from it, but other TDM phones, trunks, or IP devices in the cluster cannot call it.	Call routing is not set up correctly.	Enter the Locate commands (see “Locating Resilient Devices” on page 217) on the secondary controller to determine the status of the IP Phone. Refer to *Voice Networking -> Configure Network* in the *System Administration Tool Online Help* for instructions on the following tasks: 1. Ensure that each element in the cluster is assigned a unique CEID in its Cluster Elements form. 2. Ensure that ARS is programmed correctly to route calls to all the other elements in the cluster. 3. In the Cluster Elements form ensure that you have programmed the Feature DN fields correctly. 4. In the ICP/PBX Networking form of each element, ensure that the PBX Number matches the CEID index number that is programmed in the Cluster Elements form. 5. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone. 6. If an SX-2000 system is in the call path, ensure that the system has LW 32 Release 1.1 or later software.
		Page 4 of 6

Table 52: Troubleshooting IP Device Resiliency (continued)

Symptom	Possible Cause	Corrective Action
After the primary ICP is returned to service, the IP phones do not fail back to the primary. If an IP phone is on its secondary ICP, you hear beeps every 20 seconds, and the phone display is frozen.	The “Allow Return to Primary ICP” is set to “No” in the Controller Registry form of the primary ICP.	In the System Administration Tool on the primary ICP, navigate to the following form: System Administration->System Options-> Controller Registry Configuration. In the Controller Registry form of the primary ICP, ensure that “Allow Return to Primary ICP” is set to “Yes”.
	The duration of the health check is set too long in the Controller Registry form of the secondary ICP. The amount of time that elapses before an IP phone fails back to its primary can be quite long, depending on the health-check settings. With the default settings, after the primary ICP is back in service, the IP phones will take approximately 5 minutes to fail back.	**WARNING: Contact Mitel Customer Engineering Services. Parameters must be changed in the Controller Registry form. DO NOT change any of these parameters without consulting Mitel Customer Engineering Services.**
Message waiting indicator on a resilient phone continues flashing for a Callback message that has already been returned.	Cluster is configured to absorb routing digits.	1. In the System Administration Tool, ensure that routing digits on inbound and outbound routes are not being absorbed: - In the **Trunk Attributes form**, check how many digits are configured to be absorbed in the Dial In Trunks **Incoming Digit Modification** - **Absorb** field (should be blank). - In the **ARS Digit Modification Plans** form, check how many digits are configured to be absorbed in the **Number of Digits to Absorb** field (should be 0 (zero)) for the appropriate **Digit Modification Number**. 2. If digits are configured to be absorbed, create a new instance for the appropriate route(s) that does not absorb digits.
Hot desk user does not receive voice mail.	Voice mail is embedded in an ICP that has failed or become unreachable.	Use centralized external voice mail system.
Hot desk user logs out previous user but cannot log in.	Both primary and secondary ICPs of the resilient hot desk phone are unreachable.	Expected behavior. If both ICPs of a resilient hot desk phone are unreachable, a Logout triggers the phone to rehome. User must wait until one of the phone’s ICPs recovers and becomes reachable for the phone to be in service before they can log in to the phone.
		Page 5 of 6

Table 52: Troubleshooting IP Device Resiliency (continued)

Symptom	Possible Cause	Corrective Action
IP phones display “lost link to server” after an upgrade from 3300 Release 3.x to Release 4.0.5.1.	In 3300 Release 4.0, redirect messages were added to allow IP devices to sync to the secondary ICP for resiliency. During an upgrade from 3.x, the firmware improperly interprets the redirect message as an invalid IP address, causing phone to display “lost link to server” message.	For corrective procedure, refer to Technical Service Bulletin, “IP Sets may remain in “lost link to server” state after upgrading to Release 4.0", on Mitel Online.
		Page 6 of 6

IP Console Resiliency

Table 53: Troubleshooting IP Console Resiliency

Symptom	Possible Cause	Corrective Action
A resilient IP console is not functioning (no dial tone) after the primary controller goes out of service.	IP Console is not programmed correctly for resiliency.	Ensure that the IP console is programmed for resiliency. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for the IP console. See “IP Console Resiliency” in the *MCD Resiliency Guidelines* for details.
After an IP phone fails over to its secondary ICP, you can make calls from it, but other IP devices in the cluster cannot call it.	Call routing and ARS are incorrectly programmed.	Enter the Locate commands (see “Locating Resilient Devices” on page 217) on the secondary controller to determine the status of the IP Phone. Refer to *Voice Networking -> Configure Network* in the *System Administration Tool Online Help* for instructions on the following tasks: 1. Ensure that each element in the cluster is assigned a unique CEID in its Cluster Elements form. 2. Ensure that ARS is programmed correctly to route calls to all the other elements in the cluster. 3. In the Cluster Elements form ensure that you have programmed the Feature DN fields correctly. 4. In the ICP/PBX Networking form of each element, ensure that the PBX Number matches the CEID index number that is programmed in the Cluster Elements form. 5. Ensure that the correct secondary CEID index appears in the Remote Directory Numbers form for the resilient IP console.
Console fails back to its primary by queued calls are lost.		Ensure that ARS and call rerouting are programmed correctly.

Voice Mail Resiliency

Table 54: Troubleshooting Voice Mail Resiliency

Voice Mail Type	Symptom	Possible Cause	Corrective Action
Embedded	After an IP phone fails over to the secondary, user cannot connect to their voice mail box.	A second voice mailbox has not been configured on the secondary ICP for the resilient device.	Configure a second voice mailbox.
		Call routing on the secondary ICP is not configured to allow a user to access the voice mail ports (by dialing the hunt group number).	Ensure that call routing is set up to allow the user to access the hunt group number of the voice mail port.
		The centralized 3300 ICP embedded voice mail controller is out of service.	Check the 3300 ICP embedded voice mail server.
	Users indicate that they are missing messages.	Messages are in mailboxes on both the primary and secondary ICPs.	Instruct user to check voice mail messages in both of their voice mail boxes (user must dial different hunt group numbers to access the voice mail systems on the primary and secondary ICPs).
Centralized external	After an IP phone fails over to the secondary ICP, user cannot connect to the voice mailbox.	A voice mail box has not been configured on the external centralized voice mail controller for the resilient device.	Configure a voice mailbox for the user.
		Call routing on the secondary controller is not configured to allow a user to access the voice mail ports (by dialing the hunt group number).	Ensure that call routing is set up to allow the user to access the hunt group number of the voice mail port. Refer to the *MCD Resiliency Guidelines* for call routing configuration.
		The centralized voice mail application or server is out of service.	Check the voice mail application and server.

T1/E1 Trunk Resiliency

Table 55: Troubleshooting T1/E1 Trunk Resiliency

Symptoms	Possible Cause	Corrective Action
Users cannot make T1/E1 calls through T1/E1 MMC modules in the primary or secondary controllers.	**Links are connected in reverse**: You have programmed T1/E1 trunk resiliency correctly, but the physical connections are reversed. The Input port on the secondary controller is connected to the PSTN and the Failover port on the secondary is connected to the main port on the primary.	Reverse the connections. See "Configuring T1/E1 Trunk Resiliency" in the *MCD Resiliency Guidelines* for a configuration diagram.
The physical connections are correct and the primary controller is out of service, but users cannot make T1/E1 calls through the T1/E1 MMC on the secondary controller.	**Secondary is not programmed as resilient:** In the Digital Links form of the secondary controller, the Resiliency Link box is not checked, or you have not programmed the "Primary System Name" and "Secondary System Name".	In the Digital Links form of the secondary controller: • Select the T1/E1 link and click **Change**. Check the **"**Resilient Link" box. • From the Resilient Link ID drop-down menu, select a link identifier (1 to 4) for the secondary link. This link ID must match with the link ID that you assigned to the primary link. • Set the Primary System Name to the system name of the primary controller. • Set the "Secondary System Name" to the name of the secondary (Local) controller.
The physical connections are correct. However, alarms for the Trunk Alarm category on the secondary controller are exceeding the threshold limit. In addition, if the primary controller is out of service, users cannot make T1/E1 calls through the T1/E1 MMC on the secondary controller.	**Both links are designated as primary controller:** In the Digital Link Assignment forms of both controllers, the "Primary System Name" is set to the name of the Local controller.	
When the primary controller is out of service, the T1/E1 trunks are not transferred to the secondary controller. No alarms are generated.	**Both links are designated as secondary controller:** In the Digital Link Assignment forms of both controllers, the "Primary System Name" is set to the name of the other controller. Both controllers have their own system name selected as the "Secondary System Name".	Correct the T1/E1 trunk resiliency programming in the Digital Link Assignment forms of both systems. Refer to.the *MCD Resiliency Guidelines* for T1/E1 trunk resiliency programming.
The primary controller fails over to the secondary but users are unable to make calls through the resilient T1/E1 MMC in the secondary controller. When the user attempts to make an outgoing call, the system is unable to seize the T1/E1 trunk.	**Route List Assignment form is programmed incorrectly.** The route list programming on either the primary or secondary controller is reversed.	Correct the route list programming. Refer to the *MCD Resiliency Guidelines* for T1/E1 trunk resiliency programming.

System Data Synchronization

Sharing Operations

Table 56: Troubleshooting Sharing Operations

Symptom	Possible Cause	Corrective Action
When you click the **Sync** button in Network Elements form, you receive the following Internet Explorer script error: "Object doesn't support this property or method"	Internet Explorer security settings are preventing the synchronization.	1. In Internet Explorer, click **Tools** and then click **Internet Options**. 2. Click the **Security tab** and then click **Local internet**. 3. Click Sites and then click Advanced. 4. Add the IP address of the 3300 ICP to the zone. 5. Close all Internet Explorer windows and then relaunch Internet Explorer. 6. Log back into the 3300 Controller. 7. Access the Network Elements form, select the controller and click **Sync**.
The Start Sharing operation has not displayed any signs of progress for more than an hour (that is the operation appears to be hung).	Your Internet Explorer session is timing out before the Start Sharing operation is complete.	Install the required Internet Explorer registry file on your PC. The registry file extends your Internet Explorer session and prevents it from timing out before a Start Sharing is complete. Refer to Mitel Knowledge Base article 07-3849-01068 on Mitel Online for instructions.
Cannot start sharing with an element	SDS is not enabled on the remote element.	Ensure SDS is enabled in the System Options form of the remote element.
	Remote element not included in data sharing community.	Ensure that the remote (slave) element has been brought into the data sharing community. See "Start Sharing with a New Element" in the System Administration Tool online help for instructions. You must always bring a new element into an existing data sharing community from an element that is already in the data sharing community.
Data Sharing alarms are appearing	A minor system alarm is generated whenever an SDS data distribution error occurs.	Resolve the distribution error in the SDS Distribution Errors form. See "Resolving Pending Updates or Errors" in the System Administration Tool online help.
		Page 1 of 5

Table 56: Troubleshooting Sharing Operations

Symptom	Possible Cause	Corrective Action
Data sharing forms not appearing in System Administration menu.	SDS is not enabled on the local element.	Ensure SDS is enabled in the System Options form of the local element.
	Form is not configured as shared.	Configure the form to be shared in the SDS Form Sharing form. See “Specifying the Shared Data” in the System Administration Tool online help.
	Shared form icon does not appear beside form name in System Tool Administration menu.	After you configure forms as shared, you must log out and log back into the System Administration Tool to see the Shared form icons.
Data not being shared	Data sharing status of remote element is set to “No”.	You must start sharing with the remote element. See “Start Sharing Data” in the System Administration Tool online help.
	Scope of sharing is not set correctly.	Set the scope of the sharing. See “Identifying the Shared Data” in the System Administration Tool online help.
	Specific forms are not set as shared.	Ensure that the required forms are set to be shared. See “Identifying the Shared Data” in the System Administration Tool online help.
	Forms are set as shared but you have not started sharing with the element(s) yet at the corresponding scope.	Use the **Start Sharing** button in the SDS Form Sharing form to initiate sharing.
Data record exception is not working as expected	Record exception rules are not entered correctly.	Check to ensure that you have entered exception rules correctly. See “Specifying the Shared Data” in the System Administration Tool online help.
Unexpected application errors are being generated on the local element.	The system dimensions are not set the same across the elements. For example, one system supports 96 Classes of Service, the other element supports only 64 COS. The mismatch results in application errors.	Delete the errors and exclude the additional records from being shared. See “Specifying the Shared Data” in the System Administration Tool online help.
		Page 2 of 5

Table 56: Troubleshooting Sharing Operations

Symptom	Possible Cause	Corrective Action
Data Sharing status for the element is not consistent with all the other SDS elements in the data sharing network even after you perform a sync operation. That is, the other elements indicate in their Network Element Assignment forms that they are sharing with the element, but data is not actually being shared.	You restored an old database that had SDS disabled.	To resolve this issue: 1. At the element at which SDS is off (element A). Turn SDS on and then back off again. 2. Perform a Start Sharing operation from another SDS element (element B) in the data sharing community with element A. 3. Perform a Sync operation from element B to element A to update any data that may be out of sync on element A.
	You disabled SDS while the element was disconnected from the network.	To resolve this issue: 1. At the element at which SDS is off (element A), turn SDS on again. 2. Perform a Sync operation from another SDS element (element B) in the data sharing community with element A. Do not share any forms.
Unexpected transport errors are being generated at the local element.	The network connection between the elements is down resulting in transport errors.	Fix network issue and retry update errors.
Data Sharing Mismatch errors are being generated at the local element in the SDS Distribution Errors form.	A record has been updated on local element and sent to a remote (slave) element. The slave element has rejected the update because the slave's sharing status is out of sync with the local element (that is, the slave does not recognize that it should be sharing with the local element).	If you want the slave element to accept updates from the local element, perform a sync operation from the local element with the slave. If you want to stop sharing data with the slave element, perform a sync operation from the local element with the slave and then disable SDS at the slave element.
Unexpected Concurrent Change Rejected errors are being generated at the local element in the SDS Distribution Errors form.	Concurrent Change Rejected errors were created because during a network outage changes were made on individual elements.	Fix network issue and retry update errors.
	The shared data has different default settings because the system Country variants (set in the License and Option Selection form) are different on the master and remote elements.	Accept the values using the Force Change option, or do not share this data.
		Page 3 of 5

Table 56: Troubleshooting Sharing Operations

Symptom	Possible Cause	Corrective Action
Resilient user and device data is not being shared after you upgraded the controllers to 3300 Release 7.0 software or higher.	By default, user and device data is not shared. You must first specify the resilient user and device data that you want to be shared with the secondary elements.	Specify the resilient user and device data that you want to be shared with the secondary elements.
	Version of the remote peer has not been updated on the local controller	Perform a synchronization from the local element to the remote peer.
Data for some fields are not being shared.	If a 3300 Release 7.0 or later SDS-enabled controller is communicating with a 3300 Release 6.x SDS-enabled controller, only the forms that are supported by the Release 6.x SDS will be shared. User and device resiliency data will not be shared to the Release 6.x controller.	Upgrade the controller to the higher software level.
In the SDS Form Sharing form, some record restrictions appear as “Not supported in this Release”.	If you share the SDS Form Sharing form from a 3300 Release 7.0 controller to a controller running an earlier software release (from 3300 Release 6.1 UR2 to pre-Release 7.0) any new Release 7.0 fields that are not supported on the older software release are displayed as “Not supported in this Release” on the controller with the older software.	Upgrade the controller to the higher software level.
In the SDS Form Sharing form of a controller that has pre- 3300 Release 6.1 UR2 software, some record restrictions are incorrectly displayed as “Account Code”.	If you share the SDS Form Sharing form from a 3300 Release 7.0 or later controller among controllers that have pre-3300 Release 6.1 UR2 software, restrictions in the Feature Access Codes form may appear incorrectly. If you restrict sharing of the Call Park and Call Park Retrieve fields from the 3300 Release 7.0 system, these restrictions are incorrectly displayed as “Account Code” on the controllers with the older software.	Upgrade the controller to the higher software level.
		Page 4 of 5

Table 56: Troubleshooting Sharing Operations

Symptom	Possible Cause	Corrective Action
Errors show that data has been distributed to a network element in a way that is not consistent with the data in the Remote Directory Number form.	An administrator made an incorrect entry to the Remote Directory Number form at an element somewhere in the network and the change has been propagated by SDS.	Delete the inconsistent record from the Remote Directory Number form, and reprogram it appropriately.
On 5235 IP Phones, some application keys that are programmed on the set (for example, the History key) do not function after the set fails over or fails back from the resilient peer controller.	The Multiline Set Keys form data is shared, but the High End Set data is not shared.	In the SDS Form Sharing form, share both the Multiline Set Keys form data and the High End Set data. SDS will then share the application set key data. Instruct the 5235 IP Phone users to reprogram the application keys on their sets
A 5235 IP Phone user is unable to reprogram or clear a programmable key.	In the Multiline Set Keys form, the ”Line type” for the key is stuck at “phone apt”.	In the Multiline Set Keys form change the “line type” for the key to “Not Assigned”. The user can then reprogram the key.
Errors show that login status for a hot desk user has been improperly shared between the user's primary and secondary ICP.	A failover occurred between the time the user logged in from one device and then another. For example, an external hot desk user logs in from their cell phone, there's a failover, and before a failback can occur, they log into from their office desk phone.	Perform a sync operation from the local element to the remote peer.
There are many SDS Data distribution errors occurring on the department/location forms. Performing a Form Comparison results in conflicts for department/location. A change to the department field is not distribute throughout the network or cluster.	In a heavily congested clustered hospitality deployment, if there are a many hospitality operations being performed at the same time (either via PMS or GSA or a combination of both), then there is the possibility that department/location operations may result in distribution errors.	Perform an SDS synchronization of the department/location forms. This will update all users that reference the department/location fields with the new department/location strings.
When adding a new element to a migrated network, you receive either of the following error messages after you initiate the **Start Sharing** operation: “Synchronization failed. You must migrate this node to the new data model before attempting to join the SDS network” “Synchronization failed. The target for this operation must migrate to the new model first”.	You attempted to add a non-migrated element to the GDM network.	Follow the procedure described in “Adding an Element to the Migrated Network” in the System Administration Tool online help.
		Page 5 of 5

Sync Operations

Table 57: Troubleshooting Sync Operations

Symptom	Possible Cause	Corrective Action
The Sync operation has not displayed any signs of progress for more than one hour (that is the operation appears to be hung).	Your Internet Explorer session is timing out before the sync operation is complete.	Install the required Internet Explorer registry file on your PC. The registry file extends your Internet Explorer session and prevents it from timing out before the Sync is complete. Refer to Mitel Knowledge Base article 07-3829-00006 on Mitel Online for instructions.
Specified data has not been synchronized after you complete a Start Sharing operation.	The **Start Sharing** operation does not synchronize all the shared data across the elements. Only data in the Network Elements form and Cluster Element Definition form. It adds the element to the sharing community (member elements) and begins the sharing of data at the specified scope.	If you want to synchronize the shared system form data across the elements, you should compare the forms and then perform a **Sync** operation. See "Comparing Forms and Synchronizing Data" in the System Administration Tool online help.
Cannot sync from the local element to a remote element.	The IP addresses assigned to the elements in the Network Elements form are not unique.	Ensure that each element in the Network Elements form is assigned a different IP address.
	The system name or type for the network element on the local and remote nodes do not match.	Ensure that the same system name or type is assigned to the element in the Network Element Assignment forms of both the local and remote element.
Synchronizations take too long.	Traffic on the network is slowing the rate of record updates.	Perform the synchronization during a period of low network traffic (for example, after business hours).
	Large amounts of data are being synchronized across many elements.	Perform concurrent synchronizations to reduce the amount of time required to complete the synchronizations.
After a sync operation, large numbers of data distribution update errors appear in the SDS Distribution Errors form.	The remote element did not get the updates because the network connection to that element was down.	Fix the network issue. Retry the distribution updates. See "Resolving Pending Updates or Errors" in the System Administration Tool online help.
Many data distribution update errors appear in SDS Distribution Errors form after a concurrent sync operation.	During a concurrent synchronization, both the master and member elements reject changes coming from other network elements. Rejected changes create distribution update errors on the master element.	See "Resolving Pending Updates or Errors" in the System Administration Tool online help.
		Page 1 of 2

Table 57: Troubleshooting Sync Operations

Symptom	Possible Cause	Corrective Action
Cannot sync with the remote element (transport error).	SDS is disabled on the remote element.	Enable SDS in the System Options form of the remote element.
	Network connectivity is broken.	Fix network issue.
Synchronization fails due to a form interdependency rule violation.	A synchronization may fail if you attempt to synchronize a form before a form that it is dependent on is completed. For example, you might be unable complete the ARS Digits Dialed Assignment form until the ARS Routes form has been completed.	Synchronize the form data in order of form dependency.
Errors show that data has been distributed to a network element in a way that is not consistent with the data in the Remote Directory Number form.	An administrator made an incorrect entry in the Remote Directory Number form at an element somewhere in the network and the change has been distributed.	Delete the inconsistent record from the Remote Directory Number form, and reprogram it appropriately.
Sync operation from MCD 4.2 network element to network elements with previous releases installed fail.	The previous MCD software does not recognize the MCD 4.2 DEI (Data Entity of Interest).	Refer to Mitel Knowledge Base article 11-5191-00200.
When adding a new element to a migrated network, you receive either of the following error messages after you initiate the **Start Sharing** operation: "Synchronization failed. You must migrate this node to the new data model before attempting to join the SDS network" "Synchronization failed. The target for this operation must migrate to the new model first".	You attempted to add a non-migrated element to the GDM network.	Follow the procedure described in "Adding an Element to the Migrated Network" in the System Administration Tool online help.
After adding a new element to an SDS network, the elements have inconsistent on as (where a directory number occurs in one database but not another).	The new element contains form data which requires synchronization.	1. Access the Network Elements form on the primary element. 2. Click the check boxes beside the primary and secondary elements that you want to synchronize. 3. Click **Sync**. 4. Select the **Data Repair** option in Confirm Sync to Element. 5. Select the following form data: - Service Hosting Data - System Level Call Handling 6. Click **OK**.
		Page 2 of 2

Hunt Group or Ring Group Data Distribution Errors

Table 58: Troubleshooting Hunt Group or Ring Group Data Distribution Errors

Symptom	Possible Cause	Corrective Action
Data distribution alarm is generated. Data distribution errors related to resilient hunt groups or ring groups are displayed in the SDS Distribution Errors form.	Remote (secondary) controller does not support hunt group or ring group resiliency. The controller that you have selected as the secondary is not running the required software: Release 7 (or later) for hunt group resiliency or 3300 Release 8.0 (or later) for ring group resiliency.	Install the required software on the secondary controller, or select a different controller that is running the required software as the secondary controller. Then, delete the distribution error updates.
	Hunt group or ring group already exists on remote (secondary) controller. When you enable resiliency for a group in the Hunt Group Assignment or Ring Group Assignment form, the system adds the group data to the secondary controller. If a group with the same pilot number already exists on the secondary controller, the add group operation fails.	To fix this problem, you must • Delete the hunt group or ring group from the secondary controller and then retry the updates from the SDS Distribution Errors form, or • Disable resiliency for the hunt group or ring group, delete the corresponding error updates, and leave the two hunt or ring groups separate, or • Perform a synchronization of the hunt group or ring group data from the primary controller to the secondary controller.
		Page 1 of 2

Table 58: Troubleshooting Hunt Group or Ring Group Data Distribution Errors

Symptom	Possible Cause	Corrective Action
Data distribution alarm is generated. Data distribution errors related to resilient hunt groups or ring groups are displayed in the SDS Distribution Errors form - continued.	SDS failed to delete the Remote Directory Number (RDN) entry for the hunt group or ring group pilot number from the secondary controller's Remote Directory Numbers form. Because the RND entry could not be deleted, SDS could not update the secondary controller with the hunt group or ring group data.	Manually delete the RDN entry for the hunt group or ring group pilot number from the secondary controller's Remote Directory Numbers form. Then, retry the updates from the SDS SDS Distribution Errors form.
	Hunt group or ring group member does not exist on (remote) controller. If you add a member to a resilient hunt group or ring group and the directory number of the member is not programmed as a RDN or a device on the secondary controller, the update fails and SDS generates a distribution error.	Log into the secondary controller and program the DN of hunt group or ring group member into the Remote Directory Numbers form. Then, log into the primary controller and retry the updates from the SDS Distribution Errors form.
	A new device was added to a resilient hunt group or ring group in the Group Administration Tool. Because the member is not programmed as a RDN on the secondary controller, the update fails and SDS generates a distribution error.	
		Page 2 of 2

CHAPTER 9

LOCAL AREA NETWORK

LAN Troubleshooting Tips

- ☑ For IP Phone and physical network connectivity problems:
  - ❒Verify that the device has power.
  - ❒Verify the status of the port link integrity LEDs at each end of the cable.
  - ❒Verify that each device transmits a link integrity pulse (LINK LED on).
  - ❒If the link is down, try with another port. Verify that proper cabling is installed between the end devices.
  - ❒Verify that a crossover cable was not installed instead of a straight-though cable, and vice-versa.
- ☑ For network media problems:
  - ❒If there is excessive noise, check for cabling problems.
  - ❒If there are excessive collisions, check for duplex mismatch problems.
  - ❒For Cyclic Redundancy Check (CRC) errors, check if there is a faulty NIC or flow-control.
  - ❒If there are excessive runt frames, check for bad cables, duplex mismatches or a bad PC NIC.
- ☑ For network connectivity problems, identify the path between two end devices by doing the following PING test (in order):
  - ❒Local
  - ❒Local gateway
  - ❒Remote gateway
  - ❒Remote IP.
- ☑ There are several L2 maintenance commands that are useful for collecting details: L2 poestatus; L2 stat maclist; L2 stat port *(port summary)*; L2 stat port <portnum> *(specific port info)*; L2 stat spanning-tree; L2 stat switch. For more information, see “Using Layer 2 Statistics” on page 181.
- ☑ Maintenance and troubleshooting of your LAN/WAN network is the responsibility of your network provider. Mitel Technical Support can help you isolate minor network problems; Technical Support will escalate complex network problem to Professional Services, a billable service. Before contacting Mitel Technical Support with a LAN issue, ensure that you have the following information ready:
  - ❒network diagram
  - ❒“routeShow” command results
  - ❒results of PING test between controller and IP Phone
  - ❒“rness verify” command results
  - ❒“state xnet all” command results

LAN Troubleshooting

Table 59: LAN Troubleshooting

Symptom	Possible Cause	Corrective Action
Loss of PC network connectivity through IP phone	If your PC is connected to the network through an IP phone, your PC network connection is interrupted for approximately 1 to 2 seconds • if the IP phone momentarily loses power • if you manually reset the IP phone via the debug menu, or • if the IP phone automatically resets because it loses connectivity to the 3300 ICP for 10 minutes. Note: If a resilient IP phone fails over to its secondary controller, the PC does not lose network connectivity.	None. Connection is automatically restored in 1 to 2 seconds.

Using Layer 2 Statistics

The System Administration Tool provides various Layer 2 (L2) Ethernet traffic counters that can help with debugging LAN problems. The counters appear in the output of the “L2 Stat Port” maintenance command.

A LAN that is not operating correctly can cause IP voice quality issues ranging from minor annoyance to an inability to hold an intelligible phone call.

Incorrectly operating LANs can also cause data transfer problems for computer users such as slow response times.

The following is general information regarding LANs and what the L2 traffic parameters mean. The table at the end indicates probable causes of a particular L2 error and actions to take to try and resolve the error.

Shared versus Switched LANs

Shared LANs are LANs in which network devices share the same medium to communicate with other network devices. Examples of shared LANs are networks based on the 10Base5, 10Base2 standards or wireless LAN standards. LANs based on the twisted pair standards can also use a shared communication medium if the LAN does not support L2 switching.In shared LANs all network devices communicate on a shared medium. In the case of10Base5 and 10Base2, a coaxial cable is the shared communication media. In the case of wireless LANs, the ether or radio spectrum is the shared communication medium. In twisted pair LANs that employ ethernet hubs rather than L2 switches, the network devices communicate over a shared medium — in this instance the shared medium is the ethernet hub itself.

Some basic differences between shared LANs and switched or non-shared LANs are:

- In a shared LAN all network devices must use half duplex communication.
- In a switched LAN network devices can use half-duplex or full-duplex communication.
- In a shared LAN only one network device can transmit at any given time; otherwise, a collision will occur.
- In a switched LAN in which the network devices are configured for full-duplex operation, multiple devices can transmit simultaneously, as a result a device can transmit and receive simultaneously.
- In a shared LAN collisions are a normal occurrence. Collisions will cause alignment errors, FCS errors and, runt packets to occur on the network.
- In a switched LAN in which all network devices are configured for full-duplex operation, collisions should be minimal or non-existent. On a network that has zero collisions, it is still possible to have alignment errors, FCS errors, and runt packets due to other issues.
- As a result of the behavioral differences between shared LANs and switched LANs, the traffic counters will behave differently and error counts will have different connotations depending on whether the ICP is deployed in a shared LAN or a switched LAN.

Collisions

Shared LANs

A collision occurs on a shared LAN when two or more network devices transmit data onto the LAN at the same time. After detecting a collision the network device must abort transmitting the packet and start transmitting a jam pattern to reinforce the collision, Then, the device must wait a random period of time before attempting to re-transmit the packet. Excessive collisions can affect LAN and network device performance.

Collisions can also cause alignment errors, FCS errors and fragmented packets. The number of collisions that occur on a LAN can be related to traffic patterns on the LAN. Because of the nature of collisions, it is difficult to state what is an acceptable number of collisions and what is an unacceptable number of collisions. However, a high number of collisions on a LAN could be an indication of faulty equipment on the LAN, or it could be an indication that the LAN is too congested.

Switched LANs

On a half-duplex, twisted-pair interface, a collision occurs when receive and transmit are active simultaneously.

A twisted-pair interface that is configured for full-duplex operation allows for simultaneous transmission and reception of data. Collisions should be non-existent or minimal on LANs that are running in full-duplex mode.

CRC/FCS & Alignment Errors

When a network device transmits a packet, it appends a Cyclical Redundancy Check (CRC) to the end of the frame. The CRC value is unique for the particular packet since, like checksum generation, the data in the packet is used by the CRC generation algorithm to generate the CRC value.

If the data in the packet gets altered between the transmitting device and the receiving device, then the receiving device will detect that the packet has been altered since the CRC will not match the contents of the packet. The result is an CRC error.

A FCS error (Frame Check Sequence) is another name for a CRC error.

An alignment error occurs when a packet has an FCS error and the packet also fails to have octet alignment. When a packet has octet alignment the packet has an even byte count.

Frame Length Errors

Legal length for ethernet packets is from 64 to 1518 bytes. Ethernet packets that are shorter then 64 bytes or longer than 1518 bytes are illegal length packets and will cause the receiving device to count an error.

Any packet shorter than 64 bytes, but with a valid CRC, is considered a runt. A packet shorter than 64 bytes, but with a bad CRC, is usually considered a fragment.

A packet that has a valid CRC, and is longer than 1518 bytes, is considered a long packet. A packet that has a bad CRC and is longer than 1518 bytes is usually considered a jabber.

The following table can be used in conjunction with the L2 traffic counters to troubleshoot network problems.

Table 60: Frame Length Errors

Counter	Cause	Corrective Action
RX Discards Receive packets discarded.	Insufficient receive resources.	Contact Mitel Technical Support.
RX CRC/FCS Errors Packets received with CRC or FCS errors.	Equipment powering up or down.	No action.
	Electrical noise on the LAN.	Check for improper routing of ethernet cables
	Hardware fault on transmitting device.	Replace faulty hardware.
	Damaged/defective cable.	Replace cable.
	Bad cable termination at punch down block or at RJ-45 or RJ-71 connector.	Repair cable termination.
	Wiring plant is substandard	For 10BaseT the wire should be Cat-3 or better, for 100Base-T the wire should be Cat-5 or better.
	Duplex/speed mismatch.	Check that setting on both ends of the LAN segment are consistent.
Alignment Errors Packets received with alignment errors	See RX CRC/FCS Errors.	
RX Symbol Errors Valid length packets received that had at least one invalid data symbol.	See RX CRC/FCS Errors.	
RX Fragments Packet fragments received.	Fragments are pieces of a packet. The packet is usually fragmented due to a collision on the LAN.	Collisions and fragments are normal in a half-duplex network. Collisions and fragments should be minimal or non-existent in a full-duplex network.
RX Jabbers A jabber is a packet that is longer than 1518 bytes and has either a FCS/CRC error or an alignment error.	The jabber protection circuitry on a network device has failed. There is excessive electrical noise on the LAN.	Replace the defective network device. Check that the LAN cabling is correctly installed—e.g., cables should not be routed next to noise sources.
		Page 1 of 3

Table 60: Frame Length Errors

Counter	Cause	Corrective Action
RX Source Address Changes This count indicates the number of times that the source address (SA) has changed on packets received on this port.	A count greater than one generally indicates that this port is connected to an ethernet repeater or hub.	This is normal behavior. Note that the use of repeaters/hubs is not recommended.
RX Oversize Frames Oversize frames are packets with lengths of more than 1518 bytes that have good FCS values	Oversized frames are usually due to software bugs in applications running on network devices.	No action.
RX Undersize Frames (Runts) Undersize frames are packets with a length of less than 64 bytes that have good FCS values.	Collisions	No action required. Runts are normal when collisions occur.
	Excessive noise on the LAN	1. Check for improper cabling— e.g., ethernet cables routed too close to power lines or equipment. 2. Check cable terminations for faults. 3. Locate and replace defective network device.
TX Collisions This counter indicates the number of transmit collisions.	**Half Duplex Operation:** In a half-duplex environment collisions are normal and the rate of collisions will increase as the network traffic increases. There might be a problem in the network if the rate of collisions increases without a corresponding increase in network traffic. Practical network bandwidth utilization is about 70%. If the network is experiencing an excessive number of collisions, it could be an indication that the network is becoming congested. **Full Duplex Operation:** Collisions should be minimal in a full duplex network.	Collisions in half-duplex networks are normal. Collisions in full-duplex networks should be minimal.
Multiple Collisions This counter indicates the number of times that a transmitted packet encountered more than one collision but fewer than 16. This counter increments only if the device is in half-duplex mode.	See Excessive Collisions.	See Excessive Collisions.

Table 60: Frame Length Errors

Counter	Cause	Corrective Action
TX Late Collisions This counter indicates the number of transmit late collisions	Excessive round trip distance for packets in half-duplex networks. Network violates IEEE-802.3 standard for physical network length or there are too many (more than 3) repeaters/hubs in the network.	Ensure that network design is IEEE-802.3 compliant.
	Defective network device is not correctly sensing that the network is busy.	Locate and replace defective network device.
TX Discards The total number of transmit packets discarded.	Due to lack of transmit resources— e.g., transmit FIFO overflow, or an internal MAC transmit error.	Contact Mitel Technical Support.
Excessive Collisions This counter indicates the total number of packets that failed to be sent after 16 collisions. .	Loops in the network, e.g. more than one active network connections to the same network device.	Remove redundant network connections or enable STP/RSTP where appropriate.
	Defective network device is not correctly sensing if the network is busy.	Replace defective network device.
	Duplex mismatch.	Verify that duplex setting are consistent at both ends of LAN segment.
	Busy network.	Reconfigure network into more segments by using bridges, routers or ethernet switches.
		Page 3 of 3

CHAPTER 10

DIAGNOSING PROBLEMS

Diagnostic Tools

Table 61 lists the tools available to help you diagnose problems on a 3300 ICP system.

Table 61: Diagnostic Tools

Tool Name	Function	Location	Applies to
Alarm Details	Provides the definition and location of the alarms.	System Administration Tool. Refer to the System Administration Tool online help for instructions on how to use these tools.	3300 ICP system
Alarm Email Notification	Sends an email notification to specified personnel whenever a Minor, Major, or Critical occurs or whenever an existing alarm transitions to a different level.		
Bandwidth Statistics	Allows you to see to see real-time bandwidth usage as well as historical bandwidth statistics.		IP network
CESID Logs	Allows you to monitor and troubleshoot device moves and automatic CESID updates.		Emergency Services feature
Device Connectivity (Device Connectivity forms)	Reports previous and latest Layer 2 MAC and port number.		IP network and IP phones
IP Telephone Status (IP Telephones -All form)	Displays all of the IP telephones that are part of the system and information concerning their status.		IP phones
L2 STAT commands	Provides L2 switch ports details: MAC address, status, Spanning Tree information.		IP network
Line Measure Tool (Line Quality Measure form)	Tests to determine the line settings for Loop Start (LS) trunks that are connected to the AX Controller Card Chassis, Analog Main Board, Analog Option Board, or ASU II:		Loop Start trunks
Login/Logout Audit Logs	Allows you to identify who has accessed the system		System administration
Shared Data Update Logs	Allows you to view and manage all pending (in-progress) SDS distribution updates and update errors.		System Data Synchronization
Software and Maintenance Logs	Provides a history of the software and maintenance events.		3300 ICP system

Page 1 of 3

Table 61: Diagnostic Tools(continued)

Tool Name	Function	Location	Applies to
System Diagnostics Reporting	Allows you to collect system diagnostics information. The 3300 ICP system records diagnostic information about the system performance in a series of files. These files includes xrtc, pstswlog.db, hdrwswlog.db logs, call control statistics and other information that Mitel Technical Support can use to diagnose system problems.	System Administration Tool. Refer to the System Administration Tool online help for instructions on how to use these tools.	3300 ICP system
Voice Quality Monitoring and Statistics	Monitors voice quality for selected Mitel IP phones to identify and record: • voice quality problems requiring immediate attention • trends in voice quality performance		3300 ICP system and NetAlly tool. (Note that the NetAlly tool must be purchased separately).
IMAT	Allows you to load databases on the NSU PRI.	Maintenance or IMAT PC. See IMAT online help.	PRI/QSIG and R2 NSUs
IP Phone Analyzer	Supports IP Phone troubleshooting.	IP Phone Analyzer PC. See IP Phone Analyzer online help.	IP phones
Java Console	Supports IP Console troubleshooting.	5550 IP Console PC. To launch the Java console: at the IP Console PC, select **Start**/**Settings**/ **Control Panel**, and then click **Java Plug-in**.	5550 IP console
LEDs	Indicate overall status of unit.	Front of each unit. See “Appendix D: Status LEDs” in the *MCD Technician’s Handbook* for details.	3300 ICP hardware
	Indicate status of power supplies and RAID controller.	Back of MXe, MXe Server	3300 ICP hardware
NSU Shell	Provides NSU error messages.	NSU Maintenance Port.	All NSUs
Logviewer	Provides a history of software logs (pstswlog, xrtc, xe2t, premortem).	FTP Logs on controller (ftp from Maintenance PC). See the “View Logs” section in the “Maintenance” chapter of the *MCD Technician’s Handbook*.	3300 ICP software
			Page 2 of 3

Table 61: Diagnostic Tools(continued)

Tool Name	Function	Location	Applies to
RTC Shell	Shows error messages during the installation of the 3300. Monitors the boot sequence.	Controller Maintenance Port. See *MCD Technician's Handbook*.	3300 ICP software
Phone Configuration (Debug) Menu	Allows you to • Monitor the phone settings • Program a static IP address • Hard code connection speed and duplex mode (reboot while pressing 9) **Auto-negotiation is preferred**.	IP phones with display. See "Access Configuration Menu on Single-Mode IP Phones" on page 194 for details.	Single Mode IP phones
Dual Mode Phone Configuration (Debug) Option	Allows you to configure/view: • Network parameters • Hardware components • Set the phone mode • PIN, IP address, DHCP, Video.	5215 IP Phone (Dual Mode), 5220 IP Phone (Dual Mode, 5320 IP Phone, 5330 IP Phone, and 5340 IP Phone. See "Access Configuration Menu on Dual Mode Phones and 5235 IP Phones" on page 194.	Dual Mode IP phones
SMDR	Provides the call paths (call logs).	Controller (telnet from Maintenance PC). For MXe Server: secure telnet to System IP to use TCP/IP output streaming at RTC. See the System Administration Tool online help.	3300 ICP system
			Page 3 of 3

Phones

Diagnosing Phone Problems

No Dial Tone - Analog or DNI Phone

1. Log into the System Administration Tool and navigate to Maintenance Commands.
2. Establish the Location of the analog set using the Locate Extension maintenance command. If Locate Extension command does not work verify the programming in the Single Line DNI Sets form (analog phone) or Multiline DNI Sets form (DNI phone).
3. Run the State <extension> command. You will get one of the following responses: Idle, Busy, Manbusy, or Locked Out.

If the response is Idle:

- Connect a known good telephone set to the wiring frame.
- If the phone works then the problem is with the wiring from the frame to the set or it is the set.
- Disconnect the suspected set and connect a known good set into the terminal jack.
  - If the test set works then the faulty set should be replaced.
  - If the set does not work then the problem is in the wiring from the frame already tested or the jack.
- Check that the wiring in the jack is correct
  - If the wiring is incorrect then make the adjustment required and try the known good set again.
  - If the set still does not work then the problem is in the wiring.
- Check the wiring from the known good point at periodic intervals.

If the Response is Busy:

- Is the telephone engaged in a call?
  - If Yes then the phone is functioning normally.
  - If No then the phone is not functioning normally; take the following steps:
- Disconnect the wiring going towards the phone at the internal frame.
- Connect a known good telephone to the internal frame wiring and verify that there is dial tone.
  - If there is dial tone then there is a fault in the wiring.
  - If there is no dial tone then it could be the D-type connector (Amphenol) cable or a fault with the ASU. Verify the integrity of the Amphenol by changing it out.

CAUTION: If you change the Amphenol connector this will affect all users who are connected to that ASU.

If the Response is Manbusy:

- Find out why the circuit was busied out.
- Run the RTS <location id> command to return the circuit to service.

If the Response is Locked Out:

- Disconnect the wiring going towards the phone at the internal frame.
- Connect a known good telephone to the internal frame wiring that connects to the Analog Service unit or peripheral cabinet and verify if there is dial tone.
- If there is dial tone, then there is a fault in the wiring. If there is no dial tone:
  - For an analog phone it could be the D-type connector (Amphenol) cable or a fault with the ASU. Verify the integrity of the Amphenol by changing it out.

- For a DNI phone, it could be the a fault with the DNI card.

CAUTION: If you change the Amphenol connector on an ASU it will affect all users who are connected to that ASU.

No Dial Tone - IP Phone

1. Log into the System Administration Tool and navigate to Maintenance Commands.
2. Establish the Location of the analog set using the Locate Extension maintenance command. If Locate Extension command does not work verify the programming in the IP Set Assignment and Multiline Set Key Assignment.
3. Run the State <extension> command. You will get one of the following responses: Idle, Busy, Manbusy, or Out of Service.

If the response is Idle

- Reset the telephone.

If the response is Busy:

- Is the telephone engaged in a call?
  - If it is wait for the call to finish and check again for dial tone.
  - If the telephone is not on a call try resetting the handset.

If the response is Manbusy

- Find out why it is Manbusy.
- Return to Service using the RTS <location ID> command.

If the response is Out of Service:

- Check the phone has power (does it have a display).
  - If the phone does not have power then connect to an appropriate power source.
  - If the phone does have power then verify the link integrity LEDs.
  - A green LED on the bottom of the phone indicates a proper connection.
  - A flashing yellow LED indicates activity (data flow) on the network.

Viewing Settings and Network Parameters on IP Phones

Use the Configuration (Debug) Menu on IP Phones to view the settings and network parameters on an IP Phone. The procedures to access the configuration menu on Single Mode IP Phones and Dual Mode IP Phones are different. You can identify a Dual Mode phone by checking the label at the back of the phone. The label will specify the phone as “Dual”.

Note: The default setting from the factory is MiNet mode. The procedures described here are based on MiNet mode. The phone menus may vary in SIP mode.

Note: The Configuration Menu is not available on systems that have MLPP option selected.

Access Configuration Menu on Single-Mode IP Phones

1. Hold down both volume keys at the same time.
2. Enter **debug** (33284) on the telephone key pad (handset on hook).
3. Press **Superkey** to the display categories.
4. View details for the following categories. Press the Up/Down volume keys, or softkeys (if available) to navigate the options.
   - **Version info** (Main and Boot loads)
   - **Network** (IP information, such as the telephone's IP Address, Subnet Mask, ICP List, DHCP Server Address, TFTP Server Address, Gateway IP (Router) VLAN/Priority, DSCP)
   - **Telephony/DSP** (Telephone Directory Number and other design information)
   - **Connection** (Link Reset; Hard Reset; Toggle ERROR persistence; CDP Support; Port Settings;Static Settings)
   - **Browser Config** (Proxy Server Configuration, Debug Stream On/Off, etc.)
   - **Memory Stats** (Various design memory details)
5. Press **Phone View** or **Cancel** to exit the configuration menu.

Access Configuration Menu on Dual Mode Phones and 5235 IP Phones

Use the following procedures to configuration Dual Mode IP Phones, MiNet/SIP phones, and where specified, the 5560 IPT.

On the 5215 IP Phone (Dual Mode) and 5235 IP Phone, press ***** (yes), **0** (default), and # (no). On the 5220 IP Phone (Dual Mode), 5224 IP Phone, 5320 IP Phone, 5330 IP Phone, 5340 IP Phone, 5360 IP Phone, and Navigator press the three softkeys to select menu items.

Method A: To access the menu during the phone boot sequence:

- Hold down both volume keys until NETWORK PARAMETERS? appears.

Method A (5235 IP): To access the menu during the phone boot sequence:

- Disconnect the LAN cable from the 5235 IP Phone and then reconnect.
- Hold down the up volume key until NETWORK PARAMETERS? appears.

Method A (5560 IPT): To access the menu during the phone boot sequence:

- While powering up, hold down the Left or Right key to go into configuration mode on that side.

Method B: If the phone is up and running with the MiNet main load:

1. Hold down both volume keys at the same time.

2. Continue to hold the down volume key and release the up volume key.
3. Dial 234 on the telephone key pad and then release the down key.
   - NETWORK PARAMETERS? appears.
4. Proceed to “Viewing/Modifying Network Parameters” on page 195, “Configuring Hardware Components” on page 196, “Setting the Phone Mode” on page 197, or “Using Tools and Features” on page 197.

Method B (5560 IPT): If the phone is already up and running in dual handset mode:

1. Press and hold the Left or Right key and the Volume Up and Down down keys.
2. Release one of the volume keys, and press **234** (CFG) on the selected side.

To enter the Configuration menu on the right side while in single handset mode:

1. Press the hot prime key on the right side.
2. Hold down the Volume Up and Down keys

Method C: Using Hotkeys, at power up, press and hold the following key combinations. Note that Hotkeys access provides limited access. Methods A and B provide full access.

Note: This method is also supported on the 5560 IPT.

Table 62: Accessing the Configuration Menu: Option C

Key Sequence	Function
* and 6 (M)	Change mode to MiNet
* and 7 (S)	Change mode to SIP (Not supported on the 5560 IPT.)
7	Jump to “Config Teleworker” menu
*	Erase the PIN and VCON configuration
any other keypad keys	Display “Configure Phone” prompt

Viewing/Modifying Network Parameters

You can view and modify the following network parameters on the phone:

- Phone IP address (current and static)
- Gateway IP address (current and static)
- Subnet mask (current and static)
- Current controller IP address
- TUG1, TUG2, TUG3, and TUG4 IP addresses (current)
- TFTP server IP address (current)

- VLAN ID and priority (current and static)
- DSCP value
- IPA IP address (current and static)
- TUG IP address (static)
- TFTP SVC IP and port (static).

To view and modify network parameters:

1. Access the Configuration Menu (see page 194).
2. At NETWORK PARAMETERS?, press **Yes**. VIEW CURRENT VALUES? appears.
3. Do one of the following:
   - Press **Yes**, and then press the Up/Down volume keys to view each setting. When you return to VIEW CURRENT VALUES?, press **No**. VIEW STATIC VALUES? appears.
   - Press **No**. VIEW STATIC VALUES? appears.
4. Do one of the following:
   - Press **Yes**, and then press the Up/Down volume keys to view each setting. When you return to VIEW STATIC VALUES?, press **No**. MODIFY STATIC VALUES? appears.
   - Press **No**. MODIFY STATIC VALUES? appears.
5. Do one of the following and then reboot the phone:
   - Press **Yes**, and then press the Up/Down volume keys to scroll through each setting. Use the keypad to modify parameter(s), and then follow the prompts to store the changes and reboot the phone.
   - To reset the factory defaults, press **Default**, and then follow the prompts to set and store the factory defaults and reboot the phone.
6. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**. (On the 5560 IPT, press **Cancel** or # to reach the exit menu and then follow the display prompts.)

Configuring Hardware Components

You can configure the speed and duplex for the LAN and PC ports.

To manually configure hardware components:

1. Access the Configuration Menu (see page 194).
2. Press **No** until HARDWARE CONFIG? appears, and then press **Yes**. MODIFY SETTINGS? appears.
3. Do one of the following and then reboot the phone:
   - To modify the current hardware components, press **Yes**, and then follow the prompts to modify each setting and store the changes.
   - To reset the factory defaults, press **Default**, and then follow the prompts to set and store the factory defaults.

4. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**. On the 5560 IPT, press **Cancel** or # to reach the exit menu and then follow the display prompts.)

Setting the Phone Mode

You can program the 5215 or 5220 IP Phone (Dual Mode) to use MiNET or to work remotely using either SIP or Teleworker Solution (6010).

For SIP configuration information, refer to the 5207/5215/5220 IP Phone Installation Guide (56006499, Rev A) packaged with the phone, and to the 5215/5220 IP Phone SIP User Guide available at www.mitel.com.

Using Tools and Features

- “Erasing the Registration PIN” on page 197
- “Pinging IP Addresses” on page 197
- “Conducting a DHCP Trace” on page 198
- “Configuring Video Conferencing Parameters” on page 198
- “Restoring Factory Default Settings” on page 199.

Erasing the Registration PIN

1. Access the Configuration Menu (see page 194).
2. Press **No** until TOOLS AND FEATURES? appears, and then press **Yes**. ERASE PIN? appears.
3. Press **Yes**, and then follow the prompts to erase the PIN and to store the changes and reboot the phone.
4. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

Pinging IP Addresses

1. Access the Configuration Menu during the phone boot sequence.
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes**, and then press **No** until PING TEST? appears.
4. Press **Yes** and then follow the prompts to conduct the PING test.
5. To exit, do one of the following:
   - To return to the main menu, press **Yes** at EXIT MENU?.
   - To return to the default display, press **Superkey**.

Conducting a DHCP Trace

There is a delay while the phone performs DHCP discovery. The result of the trace displays the following information:

- Phone and Gateway IP addresses
- Subnet mask
- WINS, DNS, TFTP, ICP and Video servers
- DHCP server and Mitel IDs
- Lease
- T1 and T2
- VLAND ID and priority
- HTTP proxy
- IPA address.

To conduct a DHCP trace on the Dual Mode phone:

1. Access the Configuration Menu (see page 194).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes**, and then press **No** until DHCP Trace? appears.
4. Press **Yes**, and press the Up/Down volume keys to view the results of the DHCP trace.
5. To exit, do one of the following:
   - When you return to DHCP TRACE?, press **No**.
   - To return to the default display, press **Superkey**.

Configuring Video Conferencing Parameters

To configure video conferencing on the 5220 IP Phone (Dual Boot):

1. Access the Configuration Menu (see page 194).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** and then press **No** until VIDEO CONFIGURATION? appears.
4. Press **Yes**. VIEW PARAMETERS? appears.
5. Do one of the following:
   - Press **Yes** and then follow the prompts. When you return to VIEW PARAMETERS?, press **No**. MODIFY PARAMETERS appears.
   - To continue, press **No**. MODIFY PARAMETERS appears.
6. Do one of the following:
   - Press **Yes** and follow the prompts to modify the video conferencing parameters, store the changes, and reboot the phone.
   - To set the factory default settings, press **Default** and follow the prompts to set and store the factory defaults and reboot the phone.

7. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

Restoring Factory Default Settings

Tip: Restoring the factory default settings on the 5215 or 5220 IP Phone (Dual Mode) will erase the static network parameters.

1. Access the Configuration Menu (see page 194).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** and then press **No** until RESTORE DEFAULTS? appears.
4. Press **Yes** and then follow the prompts to set and store the factory defaults and reboot the phone.
5. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

IEEE 802.1X Authentication for IP Phones

The 5215 Dual Mode, 5220 Dual Mode, 5235, 5304, 5312 and 5324 IP Phones support IEEE 802.1X Extensible Authentication Protocol (EAP) -Message Digest 5 (MD5) Challenge authentication protocol. Refer to the 3300 ICP Engineering Guidelines for more information about this protocol.

If the network switches and their ports support 802.1.x authorization, the Remote Authentication Dial-In User Service (RADIUS) server checks the username and password of the IP phones against the entries in the database:

- If the username and password of the IP phone match the username and password on the RADIUS server, the IP phone is granted access to the port services. The IP phone boots up.
- If the username and password don't match, the IP phone is denied port access. The IP phone does not boot up.
- If a username and password are not configured for the IP phone, you are prompted to enter them.

Configuring an Authentication Username and Password

1. Power up or reboot the 5215 Dual Mode, 5220 Dual Mode, or 5235 IP Phone.
2. Wait for the prompt: PORT ACCESS CONTROL
   PRESS # TO CONTINUE.
3. Press #.
4. Enter a username of up to 20 characters in length. This username must match a name that is programmed on the RADIUS server. Use the phone keys in the table below to enter the

characters:

Table 63: DTMF Keys for entering Alphanumeric Characters

DTMF Key	Alphanumeric Characters (in order)
1	,&$!?%'"-_1
2	abc2
3	def3
4	ghi4
5	jkl5
6	mno6
7	pqrs7
8	tuv8
9	wxyz9
*	Backup and edit previous char
0	./:@0
#	Commit entered data

By default, the user name and password are entered in upper case letters. However, you can use both upper and lower case. To change to lower case, press the Volume Down key while entering a letter. All subsequent letters will be in lower case. To return to upper case, press the Volume Up key while entering a letter.

5. Press # to commit the username.
6. Enter a password from 1 to 20 alphanumeric characters in length. This password must match the password that you have programmed on the RADIUS server for the user.
7. Press # to commit the password. The message, “Waiting for 802.1X authentication” appears in the phone display.
   After the server authenticates the username and password, the IP phone boots up.

Erasing an Authentication Username and Password

1. Access the configuration menu on the 5215 Dual Mode, 5220 Dual Mode, or 5235 IP Phone. See “Access Configuration Menu on Dual Mode Phones and 5235 IP Phones” on page 194.
2. From NETWORK PARAMETERS? press **No** until on the telephone keypad until TOOLS AND FEATURES? appears.
3. Press **Yes**.
4. Press **No** until EDIT 8021X SETTINGS appears.
5. Press **Yes** ERASE 8021X DATA? appears in the display.
6. Press **Yes** to erase the current username and password.
7. Press **Yes**. The phone erases the data from its flash and then reboots.

Note: The IP phone username and password that you configured for EAP-MD5 Challenge Authentication do not need to be reprogrammed if power to the phone is lost.

Enabling or Disabling 802.1X Authentication

By default, EAP- MD5 Challenge Authentication Protocol is enabled on 5215 Dual Mode, 5220 Dual Mode, and 5235 IP Phones. If your network does not use this protocol, you do need to disable support for it on these phones.

1. Access the configuration menu. See page 194.
2. From NETWORK PARAMETERS? press **No** until on the telephone keypad until TOOLS AND FEATURES? appears.
3. Press **Yes**.
4. Press **No** until EDIT 8021X SETTINGS appears.
5. Press **Yes**. ERASE 8021X DATA? appears in the display.
6. Press **No**. If currently enabled, you are prompted to disable 8021X. If currently disabled, you are prompted to enable 8021X.
7. Press **Yes**.
8. Press Yes. The phone erases the data from its flash and then reboots.

IP Phone Boot Sequence

After you connect an IP Phone to the network, it goes through the following boot sequence (this applies to Release 5.0 and later):

Tip: MAC Addresses, and Main and Boot versions in the following table are examples for illustration purposes. The numbers displayed at the install site may be different. The x's are IP Address, VLAN, and Priority place holders.

Table 64: IP Phone Boot Sequence

Boot Sequence	Phone Display
1. Waiting for an Ethernet link to be established.	Waiting for LAN link to come up
2. If an Ethernet link is not established, continue with the bootup process.	Bad LAN link Check Ethernet cable
3. The first stage for bootup. **Note:** Refer to Table 65 on page 204 for 802.1x Port Access Control messages.	08-00-0F-AA-BB-CC Booting: 04.02.01.06
	Page 1 of 3

Table 64: IP Phone Boot Sequence(continued)

Boot Sequence	Phone Display
4. IP Phone contacts DHCP server to obtain IP address and VLAN information and a list of the controller addresses in the network. **Note:** Go to Table 66 if DHCP or TFTP fails.	Waiting for DHCP Booting: 04.02.01.06 ---------- DHCP: Discovery Booting: 04.02.01.06
5. The internal DHCP server provides one of these options: An external DHCP server provides one of these options: (where n is the number of the sub-option if encapsulation is used for the option.)	Using option 125 Using option 43 Using option 128+ - Using option 125:n Using option 43:n
6. The DHCP server on the default VLAN responds with an Offer. If Option 43 or 125 (or option 130 prior to 3300 Release 7.0) is not properly set on the server, the set awaits further Offers (n is offer number).	DHCP: Offer n Rej Booting: 04.02.01.06 ---------- DHCP: Offer n Acc Booting: 04.02.01.06
7. The set replies with a Request and the server replies with an Acknowledgement.	DHCP: Ack Booting: 04.02.01.06
8. If the data in the Ack does not contain a VLAN ID and a packet Priority value, the set retains DHCP data, jumps to Step 11.	
9. If the data included in the Ack does include a VLAN ID and packet Priority value, the set discards DHCP data and sends an untagged Release.	DHCP: Releasing Booting: 04.02.01.06 ---------- Vlan x Priority x Booting: 04.02.01.06
10.The set goes through the Discovery/Offer/ Request/Ack sequence again.The packets sent are tagged to include VLAN and Priority values supplied by the first DHCP server.	
11.The TFTP server downloads the boot image and displays the set IP address. If there is no boot image, the set jumps to Step 13. Refer to Table 67 for a description of possible error messages.	xx.xx.xx.xx Downloading
12.The boot file is copied to flash if it is a different version than the one in flash.	Upgrading Flash DO NOT POWER DOWN
13.If the boot load is the same as in flash, it is not copied.	xx.xx.xx.xx Upgrade not required
	Page 2 of 3

Table 64: IP Phone Boot Sequence(continued)

Boot Sequence	Phone Display
14.The set downloads a main image. A failure causes a phone reset, and the process starts again at step 1.	xx.xx.xx.xx Download failed ---------- xx.xx.xx.xx Downloading ---------- xx.xx.xx.xx Starting main
15.The set resets and the main load executes. The display changes to waiting for link. The set requests registration with the ICP (the first time request requires a PIN registration). The set waits for the ICP to take control.	MAIN 08.04.01.01 BOOT 04.02.01.06 ---------- Set xx.xx.xx.xx ICP xx.xx.xx.xx ---------- Waiting for ACK... ICP xx.xx.xx.xx ---------- Waiting for COMMS... ICP xx.xx.xx.xx
16.After the main boot load is downloaded, (and only when a phone in a resilient network has homed to the wrong ICP) the phone seeks out the IP address of its primary 3300 ICP from the DHCP ICP Redirect list of 3300 ICPs in the network. It is possible for the phone to be redirected and you may see this display again.	Set xx.xx.xx.xx ICP xx.xx.xx.xx ---------- Set xx.xx.xx.xx ICP xx.xx.xx.xx
17.Once communication is established, the idle display appears on the set.	<idle in service UI> <idle softkeys>
	Page 3 of 3

Table 65: IP Phone Port Access Control Sequence

Sequence	Phone Display
1. Checking the L2 switch for 802.1x Port Access Control.	Waiting for 802.1x authentication
2. With access control, the L2 switch will ask for user and password (unless the data is stored in NVRAM).	PORT ACCESS CONTROL PRESS # TO CONTINUE ---------- USER (# to end) __ ---------- PASSWORD (# to end) __
3. If Port Access Control fails.	Port Access Failure REBOOTING. . . ---------- Waiting for 802.1x authentication
4. If the data exchange succeeds or if the L2 switch does not support 802.1x Port Access Control.	Waiting for LLDP

Table 66: IP Phone Error Handling Displays

Message Description	Phone Display
Note: Check the IP Parameters (TFTP address, netmask, gateway address), to make sure that they are valid, before calling Mitel.	
If TFTP fails, usually due to incorrect TFTP Server or Gateway IP address, review IP parameters and correct errors.	RTCS creat err <number> BOOTING xx.xx.xx.xx ---------- If add err <number> BOOTING xx.xx.xx.x ---------- RTCS Bind err <number> BOOTING xx.xx.xx.x
The TFTP server sent an “I am busy” error so the phone will delay and retry.	xx.xx.xx.xx Waiting for TFTP
If the phone received a bad packet from the TFTP server, audit the TFTP server configuration and the network path.	xx.xx.xx.xx TFTP Err: <number>
This error indicates that you must review the IP parameters on the DHCP server or manually entered for the phone.	xx.xx.xx.xx TFTPerr: Packet send
Page 1 of 2Page 1 of 2	

Table 66: IP Phone Error Handling Displays(continued)

Message Description	Phone Display
Internal TFTP errors - contact Mitel Technical Support.	xx.xx.xx.xx TFTPerr: Sock create ---------- xx.xx.xx.xx TFTPerr: Sock bind ---------- xx.xx.xx.xx TFTPerr: Packet alloc
Page 2 of 2Page 2 of 2	

Table 67: Download and Software Error Displays

Message Description	Phone Display
Note: Check the IP Parameters (TFTP address, netmask, gateway address), to make sure that they are valid, before calling Mitel.	
These errors indicate that the Flash was not upgraded. The phone will pause for 3 seconds and continue.	L2 download err ---------- Boot download err ---------- L2&Boot download err
The ICP instructs the phone to get a new main executable. Two-line display set: Single-line display set:	TFTP MAIN FROM xx.xx.xx.xx ---------- TFTP MAINLOAD
If the phone received a bad packet from the TFTP server, audit the TFTP server configuration and the network path.	xx.xx.xx.xx TFTP Err: <number>
This error indicates that you must review the IP parameters on the DHCP server or manually entered for the phone.	xx.xx.xx.xx TFTPerr: Packet send
Internal TFTP errors - contact Mitel Technical Support.	xx.xx.xx.xx TFTPerr: Sock create ---------- xx.xx.xx.xx TFTPerr: Sock bind ---------- xx.xx.xx.xx TFTPerr: Packet alloc
TFTP IP address is missing from the configuration string.	125:TFTP tag missing OR 43:TFTP tag missing
ICP IP address is missing from the configuration string.	125:ICP tag missing OR 43:ICP tag missing
Page 1 of 2Page 1 of 2	

Table 67: Download and Software Error Displays(continued)

Message Description	Phone Display
Encapsulation is incorrect.	Bad 125 subopt end OR Bad 43 subopt end
Page 2 of 2Page 2 of 2	

Checking the IP Phone Resiliency Progress Display

A progress bar, consisting of flashing rectangles, is displayed in the upper right corner of the IP Phone display whenever a phone is trying to re-home (except on boot-up) to any ICP controller. The set will display a progress bar if a resilient IP phone re-homes as a result of a Hot Desk login.

Three rectangles indicate the progress of the activity:

- Left block flashing - waiting for TCP link connection with ICP
- Left block solid and middle block flashing - waiting for registration message acknowledgement from ICP
- Left and middle blocks solid, right block flashing - waiting for MiNET communications with the ICP that will take over the display at this point.

When the three rectangles are solid, the activity is complete. If the IP Phone does not complete the activity after several minutes, check the progress status by pressing the * key on the dial pad.

Table 68: IP Phone Resiliency Progress Display

Re-home Sequence	Resilient Phone Display
Resilient waiting for link UI (first block flashing)	<idle ui line1> <idle ui line2>
Resilient waiting for ACK UI (second block flashing)	<idle ui line1> <idle ui line2>
Resilient waiting for COMMS UI (third block flashing)	<idle ui line1> <idle ui line2>
Phone connected to secondary ICP (solid block)	<idle ui line1> <idle ui line2>

Diagnosing SIP Device Issues

Use the following procedure to diagnose issues with SIP line side devices that are connected to the 3300 ICP system:

1. Identify the symptoms:
   - No dial tone at SIP device?
   - Choppy or one-way audio? (See Mitel Knowledge Base article 11-5160-00010.)
   - From an internal display phone what does an internal caller see on display and hear when calling the SIP endpoint?
   - Can you ping the end point unit and the default gateway, proxies from the controller subnet?
   - TLS set takes a long time to come into service following a system reboot (Check the Registration Timer value on the set and if possible, lower the value to 5 minutes.)
2. What are the SIP end points devices?
3. What is the software revision of the devices?
4. What model of 3300 ICP controller?
5. What is the 3300 ICP software revision?
6. Gather the following Information Logs (all information is required to properly diagnose issue)
   - System Diagnostic Logs
   - WireShark trace from both endpoint and RTC of reported issue
   - Enable SIP trace on 3300 ICP to show reported issue
   - Screen captures of the end point configuration information
   - List of relative IP addresses such as 3300 ICP, end points, outbound proxies, and so forth.
7. Gather trace information with the TRACE maintenance commands:
   - To enable tracing enter SIP All TRACE ON
   - To set the trace level enter
     SIP <COMP_ID> SET LEVEL <TRACE_LEVEL>
     For example: SIP ALL SET LEVEL 3
   - To set the storage type to either the ESM or the RTC Shell, enter
     SIP <COMP_ID> SET STORAGE <TRACE_STORAGE>
     For example: SIP ALL SET STORAGE ESM
8. Enter the following SIP Maintenance Commands and collect the response (see the online help on the Maintenance Commands in the System Administration Tool):
   - SIP REGISTRAR CONTACTS ALL
   - SIP REGISTRAR CONFIG
   - SIP REGISTRAR STATS
9. For Message Waiting Indication issues, collect the data from the following commands:
   - SIP REGISTRAR CONFIG
   - SIP REGISTRAR STATS

- SIP REGISTRAR CONTACTS ALL
- SIP REGISTRAR CONTACTS <USER_NAME> (DN or ext)
- SIP MWI STATS
- SIP MWI STATS CLEAR
- SIP MWI SUBSCRIBER INFO ALL
- SIP MWI SUBSCRIBER INFO <CONTACT_NAME>

Trunks

Diagnosing Digital Trunk Issues

The following table lists key maintenance commands that you can use to diagnose issues with digital trunks. Note that the following table does not provide a comprehensive listing of all problems, but it does cover the most commonly encountered problems.

Table 69: Maintenance commands for diagnosing digital trunk issues

Symptom	Commands	Description
Any problem	edt show link config all edt show framer config all edt show link info edt show vdsu table	These commands output generic configuration information about the embedded digital trunks. From the output of these commands, you can tell how the trunks are configured. Use these commands to quickly identify any differences between the perceived and actual configuration of the trunks.
Link alarms - Part 1 (System unable to seize trunks or trunks are unavailable, network synchronization issues, and so forth)	edt show framer stats all edt show framer regs all	Outputs the statistical registers of the framers and the register settings. The outputs show exact the physical issue that is affecting the framer. You may have to dump the “framer stats” more than once as these registers change over time. Collect this output in association with the output from the “dtstats read”, “net state” and “show faults digital links” maintenance commands. **Note:** The output from these commands must be interpreted by Mitel Software Design.
Link alarms - Part 2 (Trunks not in idle when there are no calls up)	edt show vdsu alarms <plid> edt show vdsu channel <plid>	Shows the current digital trunking alarms and channel status. Use this command in conjunction with “dtstats read” and “state” commands. **Note:** The output from these commands may need to be interpreted by Mitel Software Design.
Outgoing or incoming calls rejected	edt trace vdsu namnum	Outputs the calling/called number and calling name of the call. It also displays the reason an ISDN call was disconnected (may be different than what is displayed on a set). Use this command to verify that the ARS is setup correctly and that the correct number of digits are being sent or received.
		Page 1 of 2

Symptom	Commands	Description
Call problems (dropped calls, calls getting rejected, set displays not correct, and so forth)	edt trace tsp l2l3 <plid> OR edt trace tsp cc <plid> OR edt trace vdsu cp <plid> edt trace vdsu vb <plid>	For most ISDN/QSIG problems, the “l2l3” command will be adequate. It is recommended that you turn on the “ccs” trace at the same time. For problems involving eT1D4, use the “tsp cc” command. This displays the messages to and from the T1D4 stack. If the problem is not protocol related, turn on the “cp/vb” tracing. **Note:** The output from these commands may need to be interpreted by Mitel Software Design.
Call problems are generating message output that you need to capture in a file for interpretation	edt enable logtofile (turns on message tracing) edt disable logtofile (turns off message tracing)	This command puts all of the traces turned on by “edt trace …” into the “/db/LDS_Trace.rtf” file (DigTrkTrace prior to 3300 Rls 6.1). If you need to enable tracing on a busy switch, you should send the output to the trace file because the output to the response window is slow and can impact the performance of the 3300 ICP This log file must be interpreted by Mitel designers. It is not meant to be interpreted by customers or field technicians.
T1/E1 module (embedded PRI) issues	All ESM digital trunk maintenance commands available to the NSU apply to the T1/E1 module and can be entered through the Maintenance commands form of the System Administration Tool.	Refer to Mitel Knowledge Base article 04-5191-00014
		Page 2 of 2

Hardware

Using LEDs to Diagnose Faults

Controllers, units, modules and cards have light-emitting diodes (LEDs) that indicate their current status. Refer to the Technician's Handbook for tables that list the LED states and the meaning of each state.

R2 Card Debugging

You can enter the following commands through the maintenance port of the R2 card/NSU to turn on R2 debug traces. The traces are output to the maintenance port of the R2 card/NSU. You must capture them for analysis because they are not saved to a file by the system.

Note: The baud rate for the maintenance port of the R2 card/NSU is 38400, 8N1.

Note: Most of the “r2trace” commands are a subset of the “logl3” option. Because only a subset of the logs are presented, you can focus on the R2 card debug traces.

Table 70: R2 card trace commands

Command	Purpose
option logl3	Turns on the entire R2 debug trace. The full trace can be intrusive if traffic volume is high. To toggle the debug trace off, type “option logl3” again.
r2trace all	Turns on the entire R2 debug trace. (Equivalent to option logl3).
r2trace info	Turns on R2 stack trace informational (This is a subset of option logl3
r2trace debug	Turns on R2 stack trace debug
r2trace line+	Turns on R2 stack trace line + debug
r2trace register+	Turns on R2 stack trace register + debug
r2trace call	Turns on R2 stack trace call
r2trace line	Turns on R2 stack trace line
r2trace register	Turns on R2 stack trace register
r2trace trunk	Turns on R2 stack trace trunk
r2trace pbx	Turns on R2 stack trace pbx
r2trace msg	Turns on R2 stack trace msgs
r2trace high	Turns on R2 stack high-level line + reg + pbx traces
r2trace low	Turns on R2 stack low-level line + reg + pbx traces

Table 70: R2 card trace commands

Command	Purpose
r2trace off	Turns OFF any r2trace command

Reading E2T Card Statistics

When troubleshooting network issues, you can use the **e2tshow** command to read statistics for E2T cards.

Note: For 250/700 user controllers, you will need a TAPI cable to perform this procedure. (RS232 serial cable with a PS2 connector on one end and a DB9 connector at the other.)

1. Connect to the E2T card:
   - For LX or 250/700-user controllers, connect a TAPI cable.
   - For CX, CXi, MX, or 100-user controllers, connect directly to the maintenance port.
   - For MXe/MXe Server, telnet to port 2007.
2. Enter **e2tshow**.

Note: E2T statistics accumulate over time and do not clear until the system is reset or the e2tclear command is entered. Reading the data without knowing when collection was started may be misleading. We recommend that you clear the statistics first (using e2tclear) to set a reference mark and then monitor it at regular intervals.

3. Check the output When reading the output of e2tshow, a large quantity of errors in the following categories indicates a network issue:
   - RTP Seq total missing pkts
   - RTP Seq Packets out of order
   - RTP Seq Pkts duplicate SEQ
   - Jitter Underflow
   - Jitter Overflow

The following figure shows a sample result of the e2tshow command:

```
-> e2tShow
------------------------------ E2T Stats ---
THU SEP 02 12:32:22 2004
To print the channel tables type Stream_PrintTables
TDM codec is U_LAW_CODEC -- North America
Total IP Pkts Rx    all protocols      88129
E2T Channels currently active          0 (high 2)
DSP Transcoders currently active       0 (high 0)
Local Transcoders currently active     0 (high 0)
Pass: UDP port not in voice range      12293
Info: Ch with multiple src addresses   0
Pass: ICMP_ECHOREQUEST                   0
Pass: ICMP_REDIRECT                    2
Pass: ICMP_UNREACH                     0
Drop: ICMP_UNREACH_PORT  UDP             0
Pass: ICMP_ECHOREPLY                   0
Pass: ICMP_SRC_QUENCH                    0
Pass: icmp_other                     0
Drop: Invalid DTMF digit               0
Drop: Rx UDP audio on Closed Ch          0
Drop: wrong g711 codec                 0
Drop: codec not g729                   0
Drop: codec g729 bad length              0
Drop: codec g711 bad length              0
RTP Seq  pkts with Seq skip            7
RTP Seq  total missing pkts            7
RTP Seq  Packets out of order            0
RTP Seq  Pkts duplicate SEQ              0
Host dst mod by icmp redirect            0
DTMF RTP Pkts Rx                     189
DTMF digits received                 36
DTMF no inter digit gap              0
DTMF added pkts for min len            11
DTMF short digits (corrected)          11
Jitter Underflow                   38
Jitter Starvation                  1716
EOS Detection (Active\Req\Reports)     0\0\0
Currently Active Channels

To clear the e2t counters type ->e2tclear on the console
For channel table debugging type ->Stream_PrintTables
To display MCT messages set e2tmsgtrace = 1, 0 to disable
value = 0 = 0x0
```

Figure 1: Example Result of et2show Command

Diagnosing DSP Module Related Issues

Refer to Mitel Knowledge Base article 05-5107-00004 for information on how to diagnose DSP module issues.

Use the following maintenance commands to obtain information concerning DSPs:

- DUMPDSPBOOTINFO - to display DSP resource allocation on the system.
- SHOWDSPSTATUS - to display the current status of all detected DSP MMCs on the system.

Diagnosing Formatter Card Problems

When diagnosing DS1 or CEPT Formatter Card problems:

- To obtain an indication of a link's performance over a 24 hour period, use the command: "DTSTATS READ x x x x LAST 24" (where x x x x is the cabinet, slot, shelf, link of the card).
- For the STATE command: if state is "suspect", suspect faulty card or problem with 12 volt power. If state is "not seizable", suspect 24 hour limit exceeded, relay stuck closed (test using the TEST HYBRID command), or faulty programming. The card will also appear "not seizable" for a short period after being installed.
- For the DTSTATS command: if many "number of max trans" messages, suspect incorrect Address For Message Control programming in the Digital Link Descriptors form. If "sync is absent", suspect faulty cabling, problem at the far end, or directed testing being performed at the far end. Otherwise, no sync coupled with directed hybrid test passing indicates cabling problem.
- When a formatter card is reloaded or removed, all calls that are using any channel on the card will be dropped.
- If one channel on one card is faulty, and does not affect traffic, it is not necessary to replace the card. The channel may be busied out using the BUSY command.

Note: There is no backplane cabling between the interface assembly and the DSU Card.

Diagnosing MSDN/DPNSS Link Problems

If there is a problem with the MSDN/DPNSS link:

Establish whether all calls are affected.

- If all calls are affected check the status of the link by using the DTSTAT READ PLID command.
- If the link is unavailable check the cabling. Test with a back to back cable to prove the DS1 or CEPT card.
- If the link is available check the errors.
- If some calls fail check the following:

  - ARS programming
  - Digit Conflict
  - Interconnect Restriction
  - Far end fault/programming

- If only calls to the central office fail check that the Class Of Service option of Public Network Access via DPNSS is enabled on the extension making the call and the MSDN trunks.

Loopback Testing on Digital Trunks

You can perform a loopback test on digital trunks to rule out problems with the system hardware. If two trunks can be successfully looped, and calls made that contain no slips, BERs, or framing losses, the system is operating properly. The loopback test requires the use of two trunks.

To perform loopback testing:

1. Assign a digital link descriptor to each hybrid (see the Digital Link Descriptors form).
2. Ensure the trunks are the same type. If MSDN will be used, ensure one hybrid is set to A, and the other is set to B.
3. Configure a valid Trunk Descriptor (see the appropriate CO Trunk Circuit Descriptors form).
4. Configure a valid Trunk Service Assignment (see the Trunk Attributes form), and set the Absorb field to “0”.
5. Include the trunks in two separate Trunk Groups and routes (see the Trunk Groups and the ARS Routes forms).
6. Complete ARS programming, using unique leading digits and a valid number of digits to follow (extension number length). You should be able to make a call from each Trunk Group back into the switch to a valid extension.
7. Program the Number of Digits to Absorb field, of the ARS Digit Modification Plans form, to strip away the leading digits.
8. To connect loopback between trunks on a T1/E1 Module or Network Service Unit (NSU), you have two options:
   - **Option 1**: Set one trunk in Network Termination (NT) Mode and the other trunk in Line Termination (LT) Mode. You set the line termination mode in the Link Descriptor Assignment forms of the trunks. Then, connect the trunks with a straight-through CAT5 cable.
   - **Option 2**: If you want to have both trunks in the same mode, you must wire the T1/E1 trunk connectors together as shown in Figure 2.
9. To set up loopback through the DSU card in a DSU cabinet, wire the DB15 connectors together as shown in Figure 3.
10. Complete calls to confirm there are no errors with the system equipment.

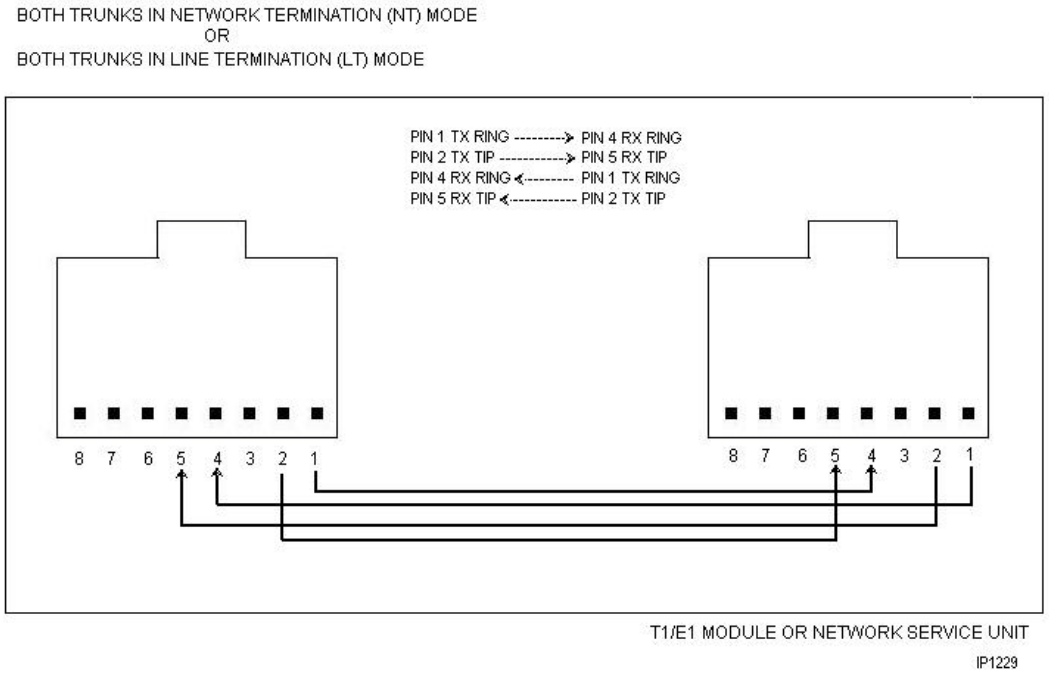


Figure 2: Loopback - T1/E1 Connectors (RJ45) on T1/E1 Module or Network Service Unit

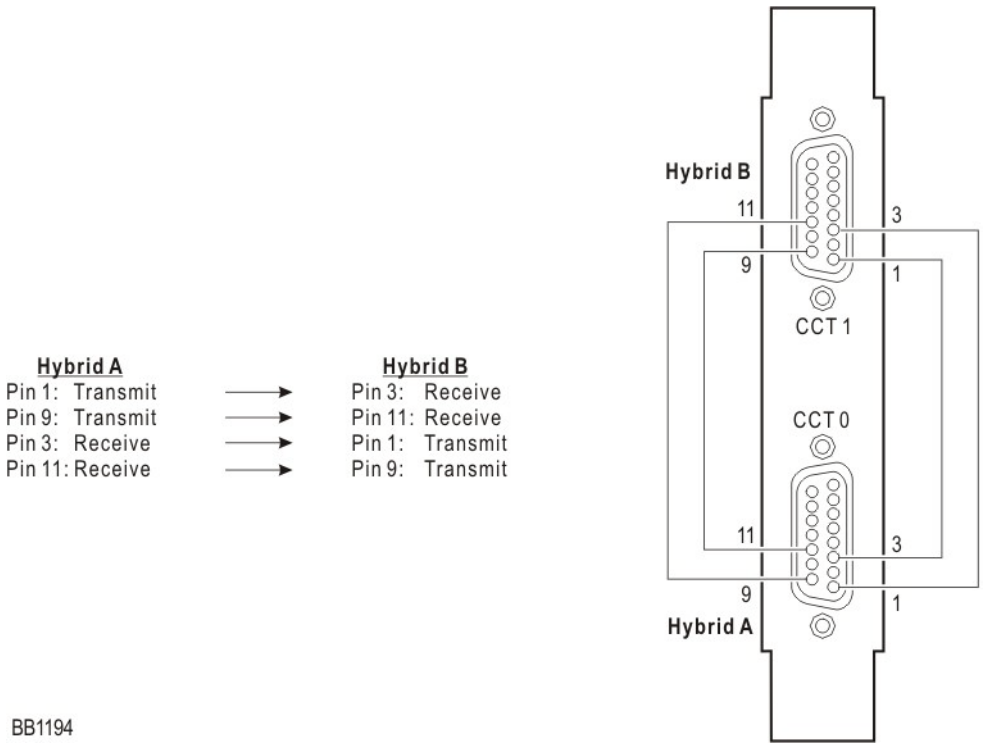


Figure 3: Loopback - Hybrid Connections (DB15 connectors on the DSU cards)

Resiliency

Locating Resilient Devices

Use the following three Locate commands to obtain information for resilient devices.

- Locate Extension
- Locate Feature
- Locate Remote

Locate Extension

You issue the Locate Extension command to acquire information about the 3300 ICP of a resilient or non-resilient extension. For resilient devices, the output of the command

- Provides primary and secondary ICP cluster element index numbers and routing digits
- Identifies the ICP the locate command was issued on (“LEID”)
- Indicates the location of the resilient device by placing an asterisk (*****) beside the primary or secondary ICP that the device is in service on

Note: To determine the state (in service, out of service, idle, busy, and so on) of the device on a given ICP, you must issue the State Extension command. For an overview of this command, see “State Extension” on page 221, and for more detailed information, refer to the *3300 ICP General Information Guide* and *3300 ICP System Administration Tool Online Help*).

Table 71. ‘Locate Extension Information for Resilient and Non-resilient Devices” p. 218 provides the input and different possible outputs for the Locate Extension command.

Table 71: Locate Extension Information for Resilient and Non-resilient Devices

Input	Output	Meaning
locate extension 1001	IP Device ID: 3 Circuit Location: 1 3 1 3 1 Extension: 1001 MAC Address: 08:00:0F:01:26:5D Primary Element: LEID 101 - Routing Digits: 2901 Secondary Element: CEID 102 - Routing Digits: 2902 *	Resilient device located on secondary ICP. Command was issued on primary ICP. LEID is the Local Element Identifier. CEID is the Cluster Element Identifier. * Indicates the known location of the device. LEID identifies the ICP that you issued the command from.
	IP Device ID: 3 Circuit Location: 1 3 1 3 3 Extension: 1001 MAC Address: 08:00:0F:01:26:5D Primary Element: CEID 101 - Routing Digits: 2901 Secondary Element: LEID 102 - Routing Digits: 2902 *	Resilient device located on secondary ICP. Command was issued on secondary ICP. * Indicates the known location of the device.
	The number refers to a remote directory number. Primary Element: LEID 101 - Routing Digits:2901 Secondary Element: CEID 102 - Routing Digits: 2902 *	Resilient device is remote and located on secondary ICP. Command was issued on an “other” ICP. * Indicates the known location of the device.
	The number refers to a remote directory number. Remote DN to CEID 101, routing digits 2901	Non-resilient device is remote and located on ICP with CEID 101 and routing digits 2901 Command was issued on an ICP that is not the device’s home element.
	IP Device ID: 3 Circuit Location: 1 3 1 3 3 Extension: 1001 MAC Address: 08:00:0F:01:26:5D	Non-resilient device is local (located on same ICP where command was issued).

Locate Feature

The Locate Feature command provides feature information in addition to the same information as the Locate Extension command (see “Locate Extension” on page 217). Table 72. ‘Locate Feature Command” p. 219 provides an example of the output provided for the Locate Feature command. Also see Table 71.

Table 72: Locate Feature Command

Example Input	Example Output	Meaning
locate feature extension 1001	IP Device ID: 3 Circuit Location: 1 3 1 3 3 Extension: 1001 Active Features: Make Busy MAC Address: 08:00:0F:00:AE:B2 Primary Element: CEID - Routing Digits: 2901 Secondary Element: LEID - Routing Digits: 2902 *	Resilient device with active Make Busy feature is located on secondary ICP. Command was issued on secondary ICP. The * indicates the known location of the phone. Local Element Identifier (LEID) identifies the ICP that you issued the command from.

Locate Remote

You issue the Locate Remote command to determine whether a device is:

- Remote and resilient
- Remote and non-resilient
- Remote and Local (both)

The following table provides possible outputs for the Locate Remote command.

Table 73: Locate Remote Command Output for Resilient and Non-resilient Devices

Example Input	Example Output	Meaning
locate remote 3001	Remote Directory Number: 3001 Primary Element: CEID 101 - Routing Digits: 2901 * Secondary Element: LEID 102 - Routing Digits: 2902	RDN 3001 is resilient DN, located on primary ICP with CEID 101 and routing digits 2901. Command was issued on the secondary ICP with Local Element Identifier (LEID) 102 and routing digits 2902. The * indicates the known location of the phone.

Page 1 of 2

Table 73: Locate Remote Command Output for Resilient and Non-resilient Devices (continued)

Example Input	Example Output	Meaning
locate remote 1001	Remote Directory Number: 1001 Primary Element: LEID 101 - Routing Digits: 2901 Secondary Element: CEID 102- Routing Digits: 2902 *	RDN 1001 is resilient DN, located on secondary ICP with CEID 102 and routing digits 2902. Command was issued on the primary ICP with LEID 101.
locate remote 1001	Remote Directory Number: 1001 Primary Element: CEID 101 - Routing Digits: 2901 * Secondary Element: CEID 102 - Routing Digits: 2902	RDN 1001 is resilient DN, located on primary ICP with CEID 101 and routing digits 2901. DN's secondary ICP has CEID 102 and routing digits 2902. Command was issued on an "other" ICP.
locate remote 3002	Remote Directory Number: 3002 Remote DN to CEID 101, routing digits 2901	RDN 3002 is non-resilient DN, located on ICP with CEID 101 and routing digits 2901.
		Page 2 of 2

Locating Resilient Hunt Groups

Use the following maintenance commands to obtain information for resilient hunt groups:

- Locate Hunt Group <pilot number>
- Locate Feature Hunt Group <pilot number>
- Locate Remote <pilot number>
- Locate Extension <pilot number>
- Locate Feature Extension <pilot number>

Table 74 lists examples of the system outputs for these maintenance commands when you issue them against a resilient hunt group.

Table 74: Locate Commands for Resilient Hunt Groups

Example Input	Example Output	Meaning
locate hunt group 4001	Pilot Number: 4001 Primary Element: LEID 201 - Routing Digits: 2905 * Secondary Element: CEID 200 - Routing Digits 2904	Hunt group pilot number 4001 is a resilient DN, located on primary ICP with local element identifier (LEID) 201 and routing digits 2905. The hunt group's secondary ICP has CEID 200 and routing digits 2904. LEID identifies the ICP that you issued the command from. The command was issued on the primary ICP. The * indicates the known location of the hunt group.

Table 74: Locate Commands for Resilient Hunt Groups

Example Input	Example Output	Meaning
locate feature hunt group 4001	Pilot Number: 4001 Active Features: Do Not Disturb Primary Element: CEID 201 - Routing Digits: 2905 Secondary Element: LEID 200 - Routing Digits 2904 *	Hunt group pilot number 4001 is a resilient DN, located on secondary ICP with local element identifier (LEID) 200 and routing digits 2904. The hunt group's primary ICP has CEID 201 and routing digits 2905. Do Not Disturb is enabled for hunt group 4001 so the hunt group is not taking calls. Command was issued on the secondary ICP.
locate remote 4001	Remote Directory Number: 4001 Primary Element: LEID 201 - Routing Digits: 2905 * Secondary Element: CEID 200 - Routing Digits: 2904	Hunt group pilot number 4001 is a resilient DN, located on primary ICP with local element identifier (LEID) 201 and routing digits 2905. The hunt group's secondary ICP has CEID 200 and routing digits 2904. Command was issued on the primary ICP.
locate extension 4001	The number refers to a Hunt Group. Pilot Number: 4001 Primary Element: LEID 201 - Routing Digits: 2905 Secondary Element: CEID 200 - Routing Digits 2904*	Hunt group pilot number 4001 is a resilient DN, located on the secondary ICP with a cluster element identifier (CEID) 200 and routing digits 2904. The hunt group's primary ICP has LEID 201 and routing digits 2905. Command was issued on the primary ICP.
locate feature extension 4001	The number refers to a Hunt Group. Pilot Number: 4001 Active Features: Do Not Disturb Primary Element: LEID 201 - Routing Digits: 2905 * Secondary Element: CEID 200 - Routing Digits 2904	Hunt group pilot number 4001 is a resilient DN, located on primary ICP with local element identifier (CEID) 201 and routing digits 2905. The secondary ICP has CEID 200 and routing digits 2904. Do Not Disturb is enabled for DN 4001 so the hunt group is not taking calls. Command was issued on an "other" ICP.

Identifying the Status of a Resilient Device

State Extension

You issue the State Extension command on an ICP to identify the state of a device that is in service on that ICP (in service, out of service, idle, busy). The State Extension command only provides information specific to the state of a given device on the ICP from which you issue the

command. For example, if you issue this command on a resilient device's primary ICP and it is out of service there, you must then issue the command on the device's secondary ICP to determine the state of that device on that ICP.

If a resilient device is out of service on both of its ICPs

- The device may, itself, be out of service.
- The device may be in the process of registering on an ICP.

State XNET ICP

You issue the State XNET ICP command to find resilient calls (calls in survival state) across IP trunks. If a device loses its ICP during a call, it retains PSTN access through a healthy controller. A healthy controller with calls on it that are in survival state is indicated in the command output by a link handle of zero.

Table 75: State XNET ICP Command Output for ICPs with Resilient Calls

Input	Output for Link Handle Value	Meaning
state xnet icp 44	0 (zero)	ICP 44 is healthy and is currently streaming calls in survival state.

Obtaining the Status of Resilient Trunks

Use the following commands to obtain the status of resilient T1/E1 trunks:

- EDT Show Resiliency
- Dtstats Read and Dtstats Clear
- Netsync State
- State
- Show Faults

Refer to the System Administration Tool online help for instructions on how to use these commands.

Controlling the Failover and Failback of Resilient Trunks

Use the following commands to control the failover and failback of resilient T1/E1 trunks:

- EDT Force Failover
- EDT Force Failback
- Programmed Failover

Refer to the System Administration Tool online help for instructions on how to use these commands.

Identifying the Current ICP

You can determine the current ICP controller for a 5140 or 5240 IP Appliance by using the phone's built in debug function.

1. Press and hold down the volume up and volume down keys.
2. Dial **33284**.
3. Release the volume up and volume down keys.
4. Select **Network**.
5. Select **ICP Server IP(s)**.

Select **Current ICP Server** to display the IP address of the current ICP controller.

Checking T1/E1 Resiliency Alarms

Trunk Alarms

If the primary controller is supporting the resilient trunks, the resilient trunks are recorded in the Trunks category of the Alarm command output. During a failover from the primary to secondary controller, the failover of the T1/E1 trunks will generate an alarm on the primary controller if the programmed trunk alarm threshold is exceeded. After the trunks fail back to the primary, the system checks the trunk alarm category to determine if the alarm threshold is still exceeded. If the trunks are operating normally on the primary, and the alarm threshold is no longer exceeded, then the system clear the trunk alarm.

During normal operation, resilient trunks that are supported by the T1/E1 Combo MMC in the primary controller are "Not Seizable" on the secondary controller. These "Not Seizable" trunks do not generate alarms on the secondary controller. Instead, the secondary controller includes the resilient trunks in the system total of the "Inactive Trunks" alarm category.

After a failover, the secondary controller controls the resilient trunks. The resilient trunks are temporarily listed in the "Trunk" alarm category of the secondary controller. After the resilient trunks fail back to the primary controller, the trunks reappear in the "Inactive Trunk" alarm category of the secondary controller.

Digital Link Alarms

On the primary controller, digital links that are associated with resilient trunks generate alarms if the links are not in a healthy state. On the secondary controller, the digital links for resilient trunks are included in the system total of the "Digital Links" alarm category.

Netsync Alarms

You can program a resilient trunk on the primary controller as a netsync source. However, do not program a resilient trunk on the secondary controller as netsync source because the system will generate a minor netsync alarm.

Typically, the alarm threshold is set such that a minor netsync alarm is generated if a netsync source is unavailable. While the resilient trunks are supported by the primary controller, the resilient trunks on the secondary controller are in a non-seizable state so the netsync source is considered unavailable. The system, therefore, generates an alarm.

Checking the T1/E1 Combo MMC Indicators

Figure 4 shows the location of the indicators on the T1/E1 Combo MMC (PN 50005160). The LEDs show the status of the link while the link is associated with the primary controller.

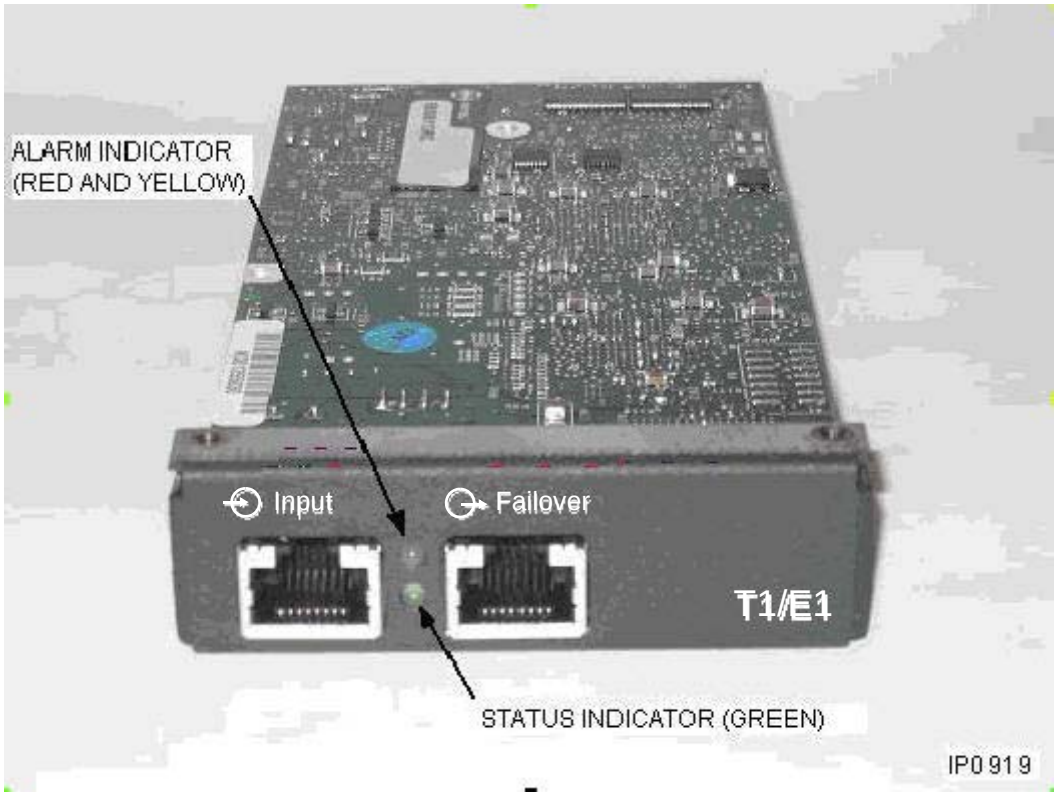


Figure 4: T1/E1 Combo MMC Indicators

Table 76 shows the meaning of the indicators. If the primary controller fails and transfers support for the trunk to the secondary controller, the LEDs on the T1/E1 Combo MMC will flash red and green.

Table 76: Meaning of T1/E1 Combo MMC Indicators (Primary Controller)

Indicators	Meaning	Action
ALARM - Off STATUS - Green	Link is functioning properly. No alarms present.	None.
ALARM - Flashing Red STATUS - Flashing Green	Primary controller has failed and the system has transferred support for the link to the T1/E1 MMC in the secondary controller.	Investigate reason for failure of primary controller. See “IP Device Resiliency” on page 159.
ALARM - Red STATUS - Off	Loss of T1/E1 signal.	Check link connection.
ALARM - Yellow STATUS - Off	No signal is being received from the PSTN.	Check link with analyzer.
ALARM - Yellow STATUS - Green	Signal from the PSTN is faulty.	Check link with analyzer.
ALARM - Off STATUS - Off	• Not programmed. Link descriptor not assigned. • System is out of service • Faulty T1/E1 MMC	Assign link descriptor. Refer to System Tool Administration online help for programming instructions.

Table 77: Meaning of T1/E1 MMC Indicators on Secondary Controller

Indicators	Meaning	Action
ALARM - Red STATUS - Off	If the primary controller is supporting the link, this alarm state on the secondary controller indicates normal operation. Because the link is not connected to this T1/E1 MMC, the alarm is not reported in the system logs of the secondary system.	None.
ALARM - Yellow STATUS - Green	Primary controller has failed and support for the link has failed over to the T1/E1 MMC in this secondary controller. However, the signal from the PSTN is faulty.	Investigate reason for failure of primary controller. See “IP Device Resiliency” on page 159. Check the link from the PSTN with analyzer.

Note: While the secondary controller is supporting the link, any link alarms that occur are shown on the secondary controller's T1/E1 MMC and reported in the logs of the secondary system. The conditions that are listed in Table 76, with the exception of the flashing Red and Green alarm, also apply to the secondary controller.

CHAPTER 11

USING LOGS

Logs

Software Logs for System Features

Feature	Error Log	Possible Cause	Corrective Action
Malicious Call Trace	Not available	The network cannot register the malicious call trace because Malicious Call Trace is not programmed on the destination node	Program destination node to support Malicious Call Trace. See the System Administration Tool online help for instructions
	User not subscribed	The Malicious Call Trace supplementary service has not been subscribed	Obtain service for Malicious Call Trace on the destination node.
	Supplementary service interaction not allowed	Some supplementary services are mutually exclusive. An MCI request cannot be sent while such a supplementary service is active	None

Hot Desking Error Logs

Feature	Error Log	Possible Cause	Corrective Action
Hot Desking	INVALID	Incorrect feature access code	Ensure the feature access code is correct. If the set is on another ICP on a cluster, ensure that the correct access codes for “Hot Desk Login”, “Hot Desk Logout”, and “Hot Desk Remote Logout” are assigned on this ICP.
	INVALID HOTDESK EXT#	Indicates that the user DN specified is invalid	Check the user DN. If the set is on another ICP on a cluster, ensure the user DN has been provisioned for the cluster.
	NOT ALLOWED	Device type does not support hot Desking	Refer to the Hot Desking topics in the System Administration Tool online help for a list of the supported sets.
		Device does not have hot desking enabled	Ensure the “Hot Desk Login Accept” field in the phone's COS is set to “Yes”
		On remote logout, indicates that the user has an active call on the phone.	The user's DN must be idle (no ringing, active, or held call) before it can be logged out.
	INVALID PIN	Indicates that the hot desk user password specified is invalid	Ensure the password is correct.
	DENIED: EXT# IN USE	On login, indicates the hot desk phone has an active call or a hot desk user is logged in and has an active call	Hot desk phone and all line appearances must be idle before a user can log in. Clear all held or active calls before logging in.
	FEATURE FAILED	In a “standalone” (non-clustered) configuration, this error may indicate that a Cluster Element ID has not been programmed for the controller. This problem may arise when a controller with an earlier version of software is upgraded to a later version.	Ensure a cluster element ID is programmed. See Program Nodal Hot Desking topic in the System Administration Tool online help for details.
		In a clustered system, a Remote hot desk user attempts to login into a registration DN that is hosted on a different controller and receives FEATURE FAILED error message.	If a remote hot desk user tries to log into a set on a controller that has a different version of software than the controller that hosts the hot desk registration DN, the feature fails. To correct this problem, upgrade the controllers to the same software version.

Voice Mail System Logs

The voice mail portion of a system log has five fields:

DATE TIME LEVEL MSG#-PORT MESSAGE

- DATE and TIME indicates when the event occurred.
- LEVEL indicates the message category and therefore the level setting required to include such messages in the output stream.
  - 0 = FATAL (voice mail system shuts down
  - 1 = ERROR (abnormal event)
  - 2 = WARNING (may be an abnormal event)
  - 3 = INFO (normal monitoring)
  - 4 = TRACE (detailed monitoring, intended for lab use only)
  - 5= DEBUG (very low-level, intended for lab use only)
- MSG# is a unique identifier for each message.
- PORT is the single-digit voice mail port associated with the message (or 0 if not port-specific).
- MESSAGE provides text indicating the event.

Error Number	Severity	Description	Solution/Action
1102 1103	ERROR	Read Error Write Error There was an error reading or writing from TRAN.DAT. This could be a one time occurrence, or it could indicate a hard drive problem.	Reboot once. If problem persists, contact service representative.
1208	WARNING	*vtlight_extn: no dextens for mailbox* **m**, *state*=**s** The MWI could not be turned on(**s**=1)/off(**s**=0) for mailbox **m** because of an invalid mailbox extension.	Check/set the mailbox extension by using the VM Mailboxes form in the System Administration Tool, or the Group Administration Tool.
1210	WARNING	vta_s9: entered undefined state The application entered a state in its state machine, which is undefined.	Contact your service representative
1216	INFO	An Administrator has logged in. The system administrators mailbox has been logged into using the BOX_ADMIN passcode	No action required.
			Page 1 of 16

Error Number	Severity	Description	Solution/Action
1219	ERROR	A privilege violation has occurred. This is a result of a Class of Service option not enabled correctly. For example, users on 5140/5240 IP Phones who wish to program their sets using the Desktop Tool must have the HCI/CTI/TAPI Call Control Allowed option set to “Yes”. This permit the user’s station to be controlled by the host computer.	Update the Class of Service options
1221	ERROR	Error calling VTGSERVICE, channel=channel Unable to start service function to initiate modem answer tone on port channel.	Contact service representative.
1502	FATAL	vtapplqh - Message Queue Memory Could Not be Allocated	Contact service representative
1504	WARNING	Message Queue file, HQ.DAT, is not opened This was a result of 2 attempts to open HQ.DAT. The first assuming the file already existed, and the second using the O_CREAT mode.	Contact service representative
1505	WARNING	Message Queue file, HQ.DAT, not initialized properly This was a result of an attempts to write to the HQ.DAT.	Contact service representative
1506	WARNING	Message Queue not updated properly from HQ.DAT The message queue file, HQ.DAT, is a backup file in case the system reboots after a message is accepted but before the message is physically delivered to the mailbox. This is a very small window. Regardless, at every boot up, we try to read this HQ.DAT file and deliver any undelivered messages. This warning occurs when the HQ.DAT file is not of the proper length. This could happen if the system was changed from a 4 port to an 8 port system.	No action required
1507	ERROR	Message Queue file, HQ.DAT, not updated properly An attempt to write to the HQ.DAT file failed during the queuing process.	Try rebooting the 3300 ICP controller. If this does not help, contact service representative
1508	ERROR	Message Queue file, %s, is not updated properly An attempt to write to the HQ.DAT file failed during the “de-queuing” process.	
			Page 2 of 16

Error Number	Severity	Description	Solution/Action
1511	ERROR	vthq: Message for mailbox mbox was not delivered: size=size There was not room in the HQ.DAT file for another record. The result of this is that a message will never be delivered. The size is the size of the queue. A message is appended to header queue in two situations: (vthq() is called to append to header queue) 1. Call is instigated from outside caller 2. Message is being sent/transferred from internal caller, and the destination mbox is locked. Messages are removed from header queue every time vtserve() (periodic service function) calls vthdq(). It de-queues a maximum of P.channel (4 in a 4 port system) every time around. vthdq() will only dequeue a message if the destination mailbox is free. Error 1511 could be manually generated by logging into a mailbox, keeping it busy and sending it more messages than header queue size. The size of header queue is dependent on P86 parameter. If this parameter is zero (default), the size of header queue was made equal to number of channels in system. We have changed the size of header queue to default to TWICE the number of channels in system. All this is done in file vtapplhq.c.	Contact service representative
1513	ERROR	*vthdq: Transaction file handle is invalid: fh*=**fh**	Contact service representative
1803	FATAL	vtappl2 - Failed to create index space	
1804	FATAL	vtappl2 - Failed to create space for names	
1808	ERROR	MASTER.DAT cannot be opened more than once at any one time	
1809	INFO	cal_get - Business hours have not been set This is an informational message that appears at reboot if the business hours have not been set by the system administrator.	No action required
1811	INFO	sg_get - No alternate greetings have been set This is an informational message that appears at reboot if there have not been any alternate greetings set by the system administrator.	
1812	INFO	MASTER.DAT was not open, but the 'close' will be executed. A request was made to close MASTER.DAT, but it was not open in the first place.	

Error Number	Severity	Description	Solution/Action
2207	ERROR	keypad table full, extra lines ignored	The keypad.tab file is too big and cannot be read completely. This should never happen and indicates a programming error. Contact service representative.
2213	ERROR	vtsrr_greet: rename(**from**,**to**) error	Unable to rename a temporary (new) greeting file to its permanent name. Try the operation again. If this still does not work, contact service representative
2214	FATAL	keypad.tab or keypad2.tab not found	Could not find keypad.tab or keypad2.tab for TUI
2215	FATAL	keypad.tab not found	Could not find keypad.tab.
2216	ERROR	vtadm_enable_disable: Can't update parm.bin While trying to enable or disable a feature, the file PARM.BIN could not be opened or written to.	Try retrieving PARM.BIN. If it is there, reboot the system and try a fresh install. If the file is not there, send a fresh version over, then try a fresh install. If this still does not work, contact service representative
2217	INFO	*vtadm_enable_disable:* Updated parm.bin	No action required
2218	ERROR	*vtadm_set_dialplan:* Can't copy master.bak	Contact service representative.
2219	ERROR	vtadm_set_dialplan: Can't restore parm.bin While trying to set the dialplan during installation, the file PARM.BIN could not be opened and/or written to.	Try retrieving PARM.BIN. If it is there, reboot the system and try a fresh install. If the file is not there, send a fresh version over, then try a fresh install. If this still does not work, contact service representative.

Error Number	Severity	Description	Solution/Action
2219	ERROR	vtadm_number_mailboxes=**errflag**, errno=**errno**	Contact service representative.
2219	WARNING	wakeup_notify_PBX:no dextens for mbox= **boxno** No extension has been configured for mailbox **boxno**.	
2229	WARNING	Write Error Rec_no=nn Write to MASTER.DAT failed.	Log the message in diag.dat and continue.
2230	ERROR	Cant update parm.bin	Contact service representative.
2403	INFO	*VT_RECDONE*:**v** Indicates that a recording has terminated. The value **v** tells how the termination happened: 2 - A terminating DTMF was detected. 5 - End of data reached (?) 7 - Timed out, rarely happens 10 - Terminated due to silence 12 - Terminated due to loop current dropping. 13 - Terminates on EOF, very rare 31 - Terminated due to non-silence; i.e. sound is constantly above a certain threshold. *VT_ON*:**v** The port has gone on-hook. *VT_OFF*:**v** The port has gone off-hook *VT_BUSY*:**v** An outdial (page) has resulted in a busy signal. *VT_NOAN*:**v** An outdial (page) has resulted in no answer. *VT_CONN*:**v** An outdial (page) has resulted in a connection being made and the recipient hears/sees the result of the page. *VT_INTER*:**v** Operator intercept&will be treated as a no answer. These are informational messages that come out to help give an idea as to the traffic of the system and how recordings were terminated. v only has meaning when on the VT_RECDONE line:	No action required

Error Number	Severity	Description	Solution/Action
3001	ERROR	vtalist:ret=**r**,total_boxes=**tb** The attempt build a list of mailbox records from MASTER.DAT failed. **r** = reason write failed: -1 = could not open MASTER.DAT -2 = could allocate space (malloc) **tb** = total number of records in MASTER.DAT	Contact service representative.
3201	FATAL	vtv40 error,file=[**filename**] The prompt **filename** cannot be found/opened.	
3207	INFO	vtspeak - Prompt **pp** File VTP.VAP Missing This means that a requested prompt could not be played. The reason is most likely that the VAP file is corrupt, this usually means truncated. If the prompt number is between 1 and 100, the file in question is VTP.VAP. If the prompt number is greater than 100, the file is VTE.VAP.	
3209	ERROR	Prompt **num** File VTP.VAP Missing Prompt number, **num**, does not exist in file VTP.VAP.	Contact service representative
3210	ERROR	MBox size incorrect File=**f** There is something wrong with the MSG file, **f**. The most likely reason is that it is full and can not accept new messages. If there is another reason, it would be shown in error message 4706	Check how many messages are in the mailbox. If OK, see message 4706.
3213	ERROR	Default Language **nnn** prompts missing, substituting English The prompts for the configured default language are not installed. English is being substituted. The value of nnn indicates the configured language: 1 = English 2 = Spanish 3 = French 4 = Dutch 5 = UK English	Select a different default language.
3214	ERROR	Alternate language **nnn** prompts missing. Language ignored. The prompts for the configured alternate language are not installed. No alternate language has been loaded. The value of nnn indicates the configured language as defined above for message 3213.	Select a different alternate language.
4001	ERROR	utxopen(path=**p**,handle->**h**)=**ret**,errno=**err**,cid=**cid** Error opening the file **p**. **cid** represents the function that called utxopen().	Contact service representative to determine if this call was for a critical file.

Error Number	Severity	Description	Solution/Action
4002	ERROR	utxclose(hd=**hd**,handle=**handle**)=**ret** Error closing file originally pointed to by hd	Contact service representative
4005	ERROR	File Handle Error	
4312	WARNING	vtxd40: Incorrect File Handle for Record The file handle passed into Record_Msg_Enter() is invalid. That is, it is less than 5 or greater than 59. This most likely means that too many files were left in the open state.	In order to get back up and running so that messages can be left, reboot the system. Then contact your service representative so that logs can be retrieved.
4313	WARNING	vtxd40: Invalid event during record d40event=event While a message was being recorded, a Dialogic event was returned that was unexpected.For details on the event, look up the event code in the Dialogic reference guide.	Note the event and contact your service representative.
4316	INFO	vtxd40: Voice Mail is gracefully shutting down This message occurs when Contact is rebooted remotely via the System Administration Tool or the Group Administration Tool.	No action required.
4319	ERROR	vtxd40: Dos Error Encountered DOS code=**c** cstate=**s** On a record or playback, there was a problem writing to or reading from the voice file. c is the _doserrno value that is set when a write, seek or read fails.	Contact service representative
4320	INFO	stopch() issued Indicates port is being stopped as part of application shutdown.	No action required
4321	INFO	T_STOP received Indicates port is being stopped as part of application shutdown.	
4323	ERROR	vtxd40: Event Error Code=**error** There was an error when calling the Dialogic get event function (**getevt**). For details on the error, look up the **error** code in the Dialogic reference guide.	Contact service representative
4324	FATAL	vtxd40: D/40 Driver Not Installed	Make sure the VOXDRV started. Watch the bootup via a serial cable and PCPlus. Otherwise, contact service representative.
4326	WARNING	vtxd40 - Unable to set Parameters Dialogic call to setxparm() failed.	Contact your service representative

Error Number	Severity	Description	Solution/Action
4327	INFO	vtxd40 - intlevel=**irq** rc=**rc** The function startsys() failed. This is because there is something wrong with the VBPC interface.	Make sure phone system is up. If problem persists, contact your service representative.
4328	INFO	vtxd40: **p** ports available, **a** installed, hourlim=**h**, vm_model_no=**m** **p** - The number of ports as indicated by the model number. **a** - The number of ports that the voice driver detected. 0 = no limit. **h** - The total number of storage hours available as indicated by the model number. 0 = no limit. **m** - This is the model number. If 0, then the model has not been set. This message is displayed on system startup, when the phone system is configured, when the fax finder is set (with phone or CGM), when a technician uses the technicians users interface to reset the ports, when the D40 token is manually sent from CGM.	No action required
4338	WARNING	vtxd40: Seek Error This seek occurs while a voice file is being queued up to be played.	If this is not an isolated incident, contact your service representative.
4341	WARNING	vtxd40: Error in Voice Code This happens when the seek error from message 4338. It should not happen for any other reason.	Contact your service representative.
4342	WARNING	vtxd40: action=**action** rc=**rc** Error occurred while trying to play a file.	Contact your service representative, noting the action and rc values.
4344	ERROR	vtxd40: Mailbox mbox unlocked for slot slot If all ports are idle there should not be any mailboxes that are locked. Therefore, this message is issued when a mailbox was unlocked.	No action required. If this happens frequently, contact service representative.
4350	WARNING	vtxd40: Call to vb_get_cpid failed vb_get_cpid() is a call to the VBPC driver that is done through a vtgservice call to the VOXDRV. To examine the exact reason why this failed, look at the VBPC log file which is located in c:\vbpc\log\vbpclog.dat.	If vbpclog.dat does not give enough information, contact your service representative.
4501	FATAL	System Parameters have FAILED to be set This can come out in the same situation as above only if there is a problem with the PARM.BIN file.	Contact service representative
4503	FATAL	vtxinit - Error starting the Voice Board	

Error Number	Severity	Description	Solution/Action
4702	ERROR	file_name=**n**, rr=**r** The message file **n** is not valid, the reason is indicated by **r**. The side affect is that any new or saved messages are lost.	No action required, the situation recovers itself.
4704	ERROR	file_name=**file**, d40derr=**error** There was an error attempting to open or write to the named file. It has to do with recording, but the actual filename dictates which part of the recording process was affected.	Contact your service representative
4706 4707 4708	ERROR	Mbox size Error ret=**ret** Mbox size Error ret=**ret** x_size_folders:Error ret=**ret**, tag=**tag** These messages occur when there is something wrong a particular mailbox MSG file. **ret** is the return value of x_size() and has the following meanings. -2 = The mailbox is full -3 = The **tag** value in the file is not correct -4 = The file handle passed in was invalid	Make sure the mailbox is not full. If not full, try renaming the MSG file. Regardless of the results of the above, contact your service representative
4907	ERROR	MBox Dir Error fname=**n** Code=**c** The message file **n** is not valid, the reason is indicated by **c**.	Contact service representative; the situation does not recover by itself.
4711	ERROR	Corrupt MBox handle=**handle** msg_no=**msg_no** ret=**ret** Playing a message failed. The reason is dictated by the return code **ret**. Below are possible values of **ret**. • Message is too short and will not be played • The actual playing of the file failed. it probably does not exist • File handle bad • The message number is bad (out of range with respect to the system wide max), or the MSG file tag is bad.	If the return code is -3 or -4, contact your service representative. If the return code is -2, it may have been purged. Otherwise, no action is required

Error Number	Severity	Description	Solution/Action
4714	ERROR	I/O Read Problem An error occurred while trying to read an MSG file. There is no reason as to why except that the amount of bytes that was read was less than what was expected.	Even though there is no extra information associated with this message, there may be other messages at the same time that indicate which file was having a problem. If this is an isolated incident, no action required. Otherwise, contact your service representative.
4715	ERROR	I/O Read Problem An error occurred while trying to **write** to an MSG file. There is no reason as to why.	Even though there is no extra information associated with this message, look at error message 4704 for the filename and associated error. Contact your service representative.
4716	ERROR	x_record:prev(.\grp\nnnnnnnn.nnn) not closed,cur=.\MSG\msgnn.vox This has only been seen with the current file being a mailbox file (msgnn.vox). The previous file has been noted to be either a grp, name, or int file - i.e. an actual message file, a name file or a greeting file. Listed below are the scenarios of when each has been reproduced. \grp • When logged into the mailbox noted in the error message, if 3 is entered to leave a memo, and the prompt begins, but the user hangs up before recording begins. • When logged into the mailbox noted in the error message, if 2 is entered to send a message, and the destination list is complete, and the prompt has begun, and the user hangs up before recording begins. \name No scenarios have been determined. \int No scenarios have been determined.	This has not been noted to cause any other problems, so no action is required by the technician.
			Page 10 of 16

Error Number	Severity	Description	Solution/Action
4717	ERROR	Previous File not closed While attempting to append to a message, there was a problem opening or writing to the existing file. This includes but is not restricted to the previous file not being closed.	If this is an isolated incident, no action required. If this continues and prevents messages from being appended to, reboot the system. If it still persists, contact your service representative.
4718	ERROR	Dir Error There is an error with the MSG file. Note that there should be other error messages with more description as to what the problem is.	Contact your service representative.
4719	Error	x_erase(%d,%d) returning %d	
4720 4721 4722	ERROR	Incorrect File Handle for Erase In all cases, a message could not be deleted due to one of the following with respect to the corresponding MSG file: • bad file handle • message number is out of range of the system default MSG tag is incorrect	Contact your service representative.
4723	ERROR	x_keep(handle,msg_no,function) returning ret This error is displayed if something goes wrong with saving a message after it has been listened to. **handle** DOS handle to the MSG file of the mailbox in question. **msg_no** - Which message do we want to keep for the mailbox in question **function** 0=Keep, 1=Mark Unread ret return value of x_keep() -1 = lseek() or read() into MSG file failed -2 = file handle bad, or bad tag in MSG file	If isolated incident, no action required. If it continues with only the same mailboxes, listen to all messages in mailbox and then delete the MSG file. Leave a new message to test. If this does not help, contact your service representative
4724	ERROR	x_stamp Corrupted Directory The attempt to time stamp a message failed because the associated MSG file did not have the proper tag inside of it.	If isolated incident, no action required. If it continues with only the same mailboxes, listen to all messages in mailbox and then delete the MSG file. Leave a new message to test. If this does not help, contact your service representative

Error Number	Severity	Description	Solution/Action
4726	INFO	deleting 0 length file: **f** This message is generated when a file that was opened to receive a recording is closed and is of zero length. For example, when leaving a message, if the user hangs up before the beep, this will leave around a zero length file. Hence when this file is deleted, the above message occurs.	No action required
4718	ERROR	x_copy(**filename**,**start**,**len**,**dfh**,**dstart**),r=**bytes_read**,w=**bytes_written** This function is used to copy parts of a message from one file to another. Mostly in the case of adding a comment to a forwarded message or appending to a message just recorded. This error occurs if the number of **bytes_read** does not equal the number of **bytes_written**. Or, if the number of **bytes_written** does not equal the **len**gth.	
4729	INFO	Msg **f** for **b** When a message is left for a mailbox, the name of the file that holds the voice data is logged. **f** - file name **b** - mailbox receiving message	No action required
4900	INFO	Application successfully initialized This message comes out every time the system is booted. It indicates that we have gotten past most initialization routines.	
4901	WARNING	Heap Problem code=**rc** Call to _heapchk() failed with a return code of **rc**.	Contact your service representative
4906	FATAL	vtxmain - System memory heap problem	
4907	FATAL	vtxmain: vtxinit failure	
4908	FATAL	Application Program Failed	
4913	INFO	MEM:main=**ms:mo**,psp=**psp** MEM,end_alloc=**ea**,malloc=**as:ao** This is an informational message for Contact Systems engineers that gives memory allocation information.	No action required
4915	FATAL	vtg_malloc(**size**) Unable to allocate memory block of **size** bytes.	Contact your service representative
4916	INFO	**ptr**=vtg_malloc(**size**) System successfully allocated **size** bytes of memory at location **ptr**	No action required

Error Number	Severity	Description	Solution/Action
5301	WARNING	File=**filename** Length=**length** The MSG file, **filename**, is greater than 10,000,000 bytes. The **length** is noted in the message	In order to get the mailbox up and running, rename the MSG file in question and then contact your service representative.
5302	INFO vta\vtutilc. ERROR vtx\vtxutil.c	Total files deleted from [**grp/msg/name**] = **n** *code* *description* -3 This means that the length of the **msgnn.vox** file is not long enough. -4 There is a special code which must be present in the file in order for the file to be valid. If that code is gone, there most likely was some sort of file corruption. The second reason this error code could come out is if enough bytes could not be read from the file. We try to read the first 5024 bytes. -5 TBD -6 TBD -7 We were unable to seek to the beginning of the file. This could also indicate a problem with the file. -8 This means there was something wrong with the mailbox file. The rc value in the error message will give you further details on what was wrong. Below is a list of the possible values for rc and what they mean: -1,-2,-3 The **msgnn.vox file** is somehow corrupt. It is not known how it could get into this state. This probably means that the **msgnn.vox file** is indicating that there are more than 250 messages.	No action requires
5303	ERROR	Copy Error **source** to **destination** code=**ret** An error occurred while copying file **source** to **destination**.	Contact your service representative
5304	INFO	vtclean: deleted **f**, age exceeded **d** days Every morning at 2:00 A.M., message files are checked to determine if their age has exceeded the configured limit. If it has, they are deleted. For each file that is deleted, this message is issued. The files name is **f** and the number of days it was checked against is **d**.	No action required
5304	WARNING	**seekid** Seek Error **fh**=fh ptr=**offset** origin=**origin** An error occurred while performing a seek on a file. Where seekid indicates who called this function.	Contact your service representative
5309	ERROR vtx\vtxutil.c	x_delete_tmsg: read error, mbox=**mailbox** This function will delete the message file that is referenced in a transaction record of the **mailbox** MSG file. Could not read the correct number of bytes from the **mailbox** MSG file.	Contact your service representative

Error Number	Severity	Description	Solution/Action
5310	ERROR	vtbox_full(Box_Num=**b**)=**r**, tot_msgs=**tm**, box_msgs=**am** fh=**fh**, f_size=**fs**, rc=**rc**, s/c=**s/c** Every time a message or memo is left for a mailbox, we first check to make sure there is room for the message/memo in the recipients mailbox. If there is not, the user is vocally informed and this message is logged. am is the maximum number of messages that the mailbox in question can contain. Note that these two messages always come out together.	The user must delete some messages before new ones can be left.
5311	ERROR	mark_erased_descriptor error=**error**, file=**box_num** An error occurred while trying to mark a descriptor file. A descriptor file is one that contains all the mailbox numbers that are to receive a group message. To determine the descriptor file, examined the mailbox MSG file. The reason the function failed is stored in **error**: 1. lseek() into the MSG file failed 2. could not read() the appropriate number of bytes from the MSG file 3. the **box_num** was not found in the descriptor file	Contact your service representative
6001	INFO	Msg **f** (**mm/dd hh:mm**) for **b** deleted A voice message sent to a single mailbox has been deleted from the disk **f** = filename, **mm** = month, **dd** = day, **hh** = hour, **mm** = minute, **b** = mbox #	No action required
6002	INFO	Msg **f** (**mm/dd hh:mm**) for **b** deleted A voice message sent to a multiple mailboxes has been deleted from the disk **f** = filename, **mm** = month, **dd** = day, **hh** = hour, **mm** = minute, **b** = mbox #	
6003	INFO	Msg **f** (**mm/dd hh:mm**) for **b** deleted A saved voice message is older than the limit specified for the mailbox. The file will be deleted when it has been erased or has exceeded the age limit for all mailboxes the message was sent to. **f** = filename, **mm** = month, **dd** = day, **hh** = hour, **mm** = minute, **b** = mbox #	
6004	INFO	Msg **f** (**mm/dd hh:mm**) for **b** deleted A voice message was saved by the mailbox owner. This message appears only the first time a message is saved. **f** = filename, **mm** = month, **dd** = day, **hh** = hour, **mm** = minute, **b** = mbox #	

Error Number	Severity	Description	Solution/Action
6005	INFO	Msg **f** (**mm/dd hh:mm**) for **b** deleted A voice message was erased by the mailbox owner. **f** = filename, **mm** = month, **dd** = day, **hh** = hour, **mm** = minute, **b** = mbox #	No action required
6006	INFO	Logged in to mailbox **b** A mailbox owner has logged in to a mailbox, b, by providing the proper mailbox/passcode combination.	No action required
6007	INFO	Mailbox **b** added The system administrator has added a mailbox, **b**, to the system.	No action required
6008	INFO	Mailbox **b** deleted The system administrator has deleted a mailbox, **b**, from the system. All associated messages and recorded greetings are deleted.	No action required
6013	WARNING	Rename from msg*.vox to msg*.vox failed	No action required. May need to restore from and to box information
6014	WARNING	Rename from nam*.vox to nam*.vox failed	
6015	WARNING	Rename from int\int*.vox to int\int*.vox failed	
6016	WARNING	Rename from int2\int*.vox to int2\int*.vox failed	
8008	WARNING	Request by CGM to seek opened file failed	Contact your service representative
8009	WARNING	Request by CGM to write to file failed This is a request to write data to the currently opened file on the Messenger side.	
8013	WARNING	Bad mailbox select location indicator: code The System Administration Tool or Group Administration Tool made a bad mailbox request. This error should never occur.	
8015	ERROR	CGM requesting too many bytes for packet size	
8016	ERROR	Request by CGM to set time of **filename** to **time** failed; errno=errno This is an attempt by the System Administration Tool or Group Administration Tool to change the time of a file on the application side. This is a very obscure request and is rarely done.	
8017	WARNING	Bad mailbox command: **errno** This is an attempt by the System Administration Tool or Group Administration Tool to issue a command that is not valid.	Take note of the error, and contact your service representative
			Page 15 of 16

Error Number	Severity	Description	Solution/Action
8201	WARNING	Trying to shift a negative number of bytes This is an error that can occur during the communications protocol. It should never happen.	Contact your service representative
8301	WARNING	Bad return value from 'valid_packet()'	No action required.
			Page 16 of 16

Index

SYMBOLS

37

NUMERICS

404 page not found 136
5140 IP phone, web browser error 61
5224 IP phone, display stuck 62
5235 IP phone, apps not functioning 60
5235, 5320, 5330, 5340, 5360 IP phones, loss of apps 60
5240 IP phone, web browser error 61
5310 conference unit, not working 62, 65
5422 PKM, one way audio 62
5560 IPT, handset issues 59
5702 IP phone issues 60

A

Accessing
  electronic documentation 3
  Mitel online 3
  product support 15
  support 15
  telephone support 15
ACD, troubleshooting 140
Add held 98
Addressing technical issues 5
Advice of charge 98
After hours telephone support 10
After-hours calls, definition 19
Alarm details 189
Alarms
  hardware 36
  troubleshooting 37
Alignment errors 182
Alpha tagging 98
AMC, unable to communicate with 29
Analog service unit
  ONS circuit 46
  troubleshooting 46
Analog trunk troubleshooting 115
ANI/DNIS/ISDN number delivery trunk 117, 119
Application Management Center, unable to communicate with 29
Application reach through 157
Applications
  missing from 5235, 5330,5340 IP phones 60
  not functioning on 5235 IP phone 60
ASU
  ONS circuit 46
  troubleshooting 46
Audio
  broken 79
  distorted 79
  file download troubleshooting 139
  issues after upgrade 81
  Issues appear after upgrade 81
  one-way 78
  poor quality on LS trunks 116
  quality problems 78
AudioCodes Mediant 1000 47
Auto answer 99
Automatic call distribution 140
AX troubleshooting 25

B

Backups, troubleshooting 90
Balanced network setting 116
Bandwidth management 155
Bandwidth statistics 189
Bit error rate 118
Boot failure, IP phones 62
Boot sequence, IP phones 201
BRI troubleshooting 123
Broadcast storms 18
Broken audio 79
Browser
  required for accessing docs 4
  required for Mitel online 3
Business hours, of support 19

C

Call forwarding 100
Call history 101
Call pickup - clustered 102
Call pickup - directed 101
Call, making a support call 19
Calling line identification 117
Calling product support 15
Camp-on 102
CAT 5 18
CCS TRACE maintenance command 122
CEPT or DS1 card links fail 126
Certificate, of security 134
CESID logs 189
Charges, for support 12

CITELlink gateway 47
CLASS/CLIP 47
Clear all features 102
CLID 117
Clustering, troubleshooting 155
Collisions 182
Compression
  affects on audio quality 79
  DSP status 37
Conference 102
Conference split 103
Conference unit, not working 62, 65
Configuration menu 18
Configuration menu, on IP Phones 194
Connection, of phone 77
Console
  resiliency 165
  troubleshooting 82
  unable to access on MXe server 28
Consultation credits 9
Controller
  not powering up 25
  unable to establish communication 26
Cookies, disabled in browser 132
CRC/FCS 182
Credits, consultation 9
Crossover ethernet cable 26
CX/CXi troubleshooting 25

D

DASS II
  circuit fails to return to service 120
  link does not work 119
Database, loss of 87
Debug menu
  and MLPP feature 69
  on IP Phone 194
  on IP phone 18
Desktop user tool, troubleshooting 139
Device connectivity forms 189
DHCP server
  and IP phone issues 69
  discovery issues 71
  server corrupted 70
  troubleshooting 26
DHCP trace, for dual mode phones 198
Diagnosing
  digital trunk issues 209
  hardware 211
  phone problems 191
  R2 card debugging 211
  SIP device issues 207
  using LEDs 211
Diagnostic and maintenance forms 35
Diagnostic tools 189
Dial tone, none 77
Digital link alarms 223
Digital trunk troubleshooting 118
Direct page 104
Discontinued products 11
Discovery issues, DHCP server 71
Display phones, troubleshooting 56
Distorted audio, on NSU 79
DMS500 switch 120
Do not disturb 105
Documentation, supporting 3
DS1 or CEPT card links fail 126
DSP card or module 51
DSP module
  diagnosing problems 214
  troubleshooting 37
DSP status
  command 37
  troubleshooting 37
DSP status command 37
DSS/BLF key 105
DSU cabinet
  faulty triple FIM 49
  troubleshooting 49
DTSTATS command 214
Dual Framer (T1/E1) module 51
Dual mode phone, Configuration (Debug) option 191
Dual Mode phone, fails to boot up 59

E

E2T
  card statistics 212
  does not come up 26
  ICP communication alarm 36
e2tshow 212
E911 support 141
Echo
  between IP and TDM phones 80
  between IP phones 81
  on ASU voice calls 46
edt commands 209
e-mail notification
  of alarms 189

of new articles 10
Embedded
BRI troubleshooting 123
modules 50
PRI troubleshooting 121
resilient device support 168
voice mail 142
Emergency
calling 141
calls for support 20
Erasing phone registration PIN 197
Essential
environments 20
services 20
Excessive
bit error rate 118
slips 118
Export button, fails to launch Excel spreadsheet 137
Exporting data, unable to open spreadsheet 111
External forwarding 119

F

Fail
to load file 88
to log in 88
Failed out of box, replacement 11
Failover, of resilient trunks 222
Fan alarm 37
Fax
finder (voice mail option) 238
general troubleshooting 17
server 119
service profiles 157
tone 144
Feature key 105
Features
A to B 98
add held 98
advice of charge 98
alpha tagging 98
auto answer 99
C 100
Call forwarding 100
call history 101
call pickup - clustered 102
call pickup - directed 101
camp-on 102
clear all features 102
conference 102
conference split 103
D to G 104
direct page 104
do not disturb 105
DSS/BLF key 105
feature key 105
forwarding 100
group page 106
H to L 107
handset receiver volume 107
handsfree operation 107
hold 107
hunt group 107
language change 108
loudspeaker paging 108
M to O 108
message waiting indication 108
music on hold 109
P to R 110
private line automatic ringdown 110
record a call 110
ring groups 110
Speed call 111
telephone directory support 111
transfer 111
troubleshooting 97
trunk answer from any station 111
Field replaceable units, returning 21
Firefox
cookies (enabling) 132
dialog boxes in Sys Admin Tool stuck open 134
security certificate (installing) 134
unable to connect to MCD-ISS 133
Flowchart, for resolving issues 5
Formatter card, diagnosing problems 214
Forwarding 100
Forwarding, of ext incoming PRI call 119
Frame length errors 182
Frequency-Shift Keying 56
FRUs 21

G

Gateways, troubleshooting 47
Generic group alert key 140
Group page 106, 129
Groups - key system and multicall 106

H

Handset receiver volume 107

Handsfree operation 107
Hardware
  alarms 36
  diagnosing problems 211
  returning faulty hardware 21
  tips for troubleshooting 35
Headset issues, IP phones 60
Hold 107
Hot desking 141
Hunt groups
  troubleshooting 107
Hunt groups, locating resilient 220
Hyperterminal 28

I
i-Button 29
Identifying current ICP 223
IEEE 802.1X Authentication, for IP phones 199
IMAT
  tool 190
IMAT troubleshooting 139
Indicators, on T1/E1 combo MMC 224
Initial setup, troubleshooting tips 25
Invalid VLAN ID 70
IP address, maintenance PC (MXe, CX or CXi) 26
IP console
  resiliency 165
  troubleshooting 82
IP device, port status LEDs off 66
IP networking 129
IP phone
  analysis 19
  analyzer 190
  audio quality, troubleshooting 78
  collecting problem details 18
  DTMF keys for alphanumeric characters 200
  fails to boot 57, 62
  headset issues 60
  IEEE 802.1X authentication 199
  info 35
  locked-out 58
  no data link 67
  pin in memory 58
  Power inactive LED on 67
  power inactive LED on 68
  power troubleshooting 65
  resiliency progress 206
  resiliency progress display 206
  resiliency troubleshooting 159
  troubleshooting 56
  troubleshooting connections 77
  troubleshooting registration 69
IP telephone status 189
IP trunks, troubleshooting 129
IPA 19
ISDN maintenance and admin tool 139

J
Java console 190

K
KeepAlives 19
Knowledge base
  checking 12
  description 9

L
L2 maintenance commands 179
L2 STAT commands 189
LAN, troubleshooting 179
Language change 108
Layer 2 statistics 181
LED status 16
LEDs 190
Licensing
  cannot move licenses 29
  MAP licensing 30
  troubleshooting 29
Line measure tool 189
Line termination (LT) mode 215
Link, waiting for 74
Load failure, TFTP 74
Local area network, troubleshooting 179
Locating resilient devices 217
Log viewer 190
Login/Logout audit logs 189
Logs
  for login/logout 189
  hot desking 230
  software 229
  voice mail system 231
Loopback testing, on digital trunks 215
Loss of system database 87
Loudspeaker paging 108
LS trunks, poor quality audio 116

M

Maintenance and diagnostic forms 35
Managed Application Server application 28
Management Access Point, license reminder 30
Management tools, troubleshooting 132
Manufactured discontinued products 11
Message waiting indication 108
Methodology, troubleshooting 3
MG Comms alarm, MXe Server 37
Migration issue, peripheral cabinet 48
Mitel Knowledge Base
  checking 12
  description 9
Mitel Mezzanine Card, info 35
Mitel online
  accessing 3
  browser requirements 3
Mitel Technical Support, phone numbers 19
MNM 156
Modules, troubleshooting 50
MSDN/DPNSS
  diagnosing link problems 214
  link troubleshooting 125
Multi-node management 156
Music on hold 109
MXe
  hardware status command 38
  hardware troubleshooting 38
  troubleshooting 25
MXe Server
  fails to boot 41
  Linux logs 93
  no operating server 43
  serial login fails 42
  suspected APC failure 42
  troubleshooting 41
  troubleshooting setup 28

N

Netsync alarms 223
Network ICMP Redirect Packets 58
Network parameters, view and modify from phone 195
Network service unit, troubleshooting 44
Network Termination (NT) Mode 215
Networked voice mail 149
No dial tone 77
Non-unique match error 135
Norstar phones, fail to register 62
Notification, of new Technical Bulletins 10
NSU
  does not come into service 119
  shell 190
  troubleshooting 44

O

One-way audio 78
Online service desk 8, 9, 10, 13
ONS sets, troubleshooting 56
OSD 8, 9, 10, 13
Out of box, failures 11
Overview, of technical support 8

P

Page not found error 136
Password reset 10
Patches, software 10
Peripheral cabinet
  migration 48
  migration troubleshooting 47
  troubleshooting 47
Phantom
  calls 55
  ringing 141
Phone
  audio quality 78
  connection problems 77
  display, checking for resiliency status 206
  numbers, of Mitel product support 19
  troubleshooting connection 77
Phone-Feature matrix 97
Phones
  Calls being cut off 54
  configuring LAN and PC ports 196
  general phone issues 51
  no busy signal 54
  phantom calls 55
  setting IP Phone mode 197
  volume setting lost 55
PING
  test 179
PLAR 110
PoE 18
Power
  IP phones 65
  over Ethernet 18
PRI troubleshooting 121
Private line automatic ringdown 110
Problem

definition 16
resolving technical issues 5
symptoms 16
Problem details
collecting for phone 18
collecting info 16
Product support, accessing 15
PSTSWLOG 17

R

R2 card debugging 211
R2 setup issue 124
r2trace commands 211
RAD ports, don't play for incoming calls 140
Real Time Controller, info 35
Record a call 110
Registering
for technical support services 9, 13
Registration
invalid VLAN ID 69, 70
TFTP load failure 74
troubleshooting IP phones 69
Regproc trap 75
Releases, software 10
Requirements, for doc access 4
Resiliency
checking T1/E1 alarms 223
identifying the current ICP 223
IP console 165
locating devices 217
progress display, on IP phones 206
troubleshooting 159
trunk status 222
Resilient trunks
failover/failback commands 222
Resolving technical issues 5
Restores, troubleshooting 90
Ring groups 110
RTC
flash 41
shell 191

S

SDS, troubleshooting 168
Security certificate issues 134
Self help solutions 12
Service charges, summary 12
Setup, troubleshooting tips 25
Shared data update logs 189
Shared LAN 181
Sharing operations 168
Show Status
DSP 37
Redundant 38
Single-line set, troubleshooting 56
SIP
access Configuration Menu on dual mode SIP sets 194
ACD RAD ports don't play 140
audio issues 81
diagnosing SIP device issues 207
phone registration failure 59
SMDR 151
trunk troubleshooting 130
Slips, excessive 118
SMDR 151, 191
Sniffer 18, 19
Software
installation and upgrade 88
patches 10
releases 10
troubleshooting 87
unable to download 87
Software and maintenance logs 189
Software installer tool, troubleshooting 138
Solaris X 152
Solutions, self help 12
Specific phone models, troubleshooting 59
Spectralink wireless issues 60
Speed call 111
Spreadsheet, unable to open 111
Standard telephone support 10
State extension, command 221
State XNET ICP, command 222
Station message detail recording 151, 191
Statistics, bandwidth 155
Statistics, layer 2 181
Status indicators 190
Status, of a resilient device 221
Straight-through ethernet cable 26
Summary of service charges 12
Sun Ray, troubleshooting 152
Superset 4000, headset issues 60
Support call, making 19
Support, standard telephone 10
Switched LAN 181
Sync operations 173
System data synchronization, troubleshooting 168

System identifier 16, 29
System management tools, troubleshooting 132

T

T1 trunk unstable 119
T1/E1 combo MMC indicators 224
T1/E1 resiliency alarms 223
T1/E1 trunk resiliency
  controlling failover/failback 222
  status of trunks 222
  troubleshooting 167
TBs 9
Technical
  bulletins 9
  issues, resolving 5
  services 15
  support network 8
Technical support
  available services 9
  charges 12
  identification code 9
  list of products 11
  registering 9, 13
Technical support network, description 8
telephone directory support 111
Telephone support
  after hours 10
  obtaining 15
  standard 10
Tenovis PBX 120
TFTP fail 76
TFTP load failure 74
Tickets, technical support 8
Tools, diagnostic 189
Transfer 111
Troubleshooting
  analog service unit 46
  analog trunks 115
  audio file downloads 139
  automatic call distribution 140
  backups and restores 90
  bandwidth management 155
  clustering 155
  controllers 25
  desktop user tool 139
  digital trunks 118
  DSU cabinet 49
  E911 support 141
  embedded BRI 123
  embedded modules 50
  embedded PRI 121
  embedded voice mail 142
  gateways 47
  hardware 35
  hot desking 141
  IMAT 139
  initial setup 25
  IP console 82
  IP trunks 129
  LAN 179
  licensing 29
  methodology 3
  MSDN/DPNSS links 125
  Multi-node management 156
  MXe Server 41
  NSU 44
  peripheral cabinets 47
  Phone audio quality 78
  phone boot sequence 201
  phone connection 77
  phones 51
  resiliency 159
  SDS 168
  SIP trunks 130
  SMDR 151
  software installer tool 138
  specific phone models 59
  system features 97
  system management tools 132
  system software 87
  T1/E1 trunk resiliency 167
  telephone directories 166
  trunks 115
  voice mail resiliency 166
  voice networking 155
  XNET trunks 127
Trunk alarms 223
Trunk answer from any station 111
Trunk calls, not receiving 115
Trunk resiliency, status of trunks 222
Trunks
  digital trunk troubleshooting 118
  ring not heard immediately 116
  troubleshooting 115
  unable to dial out 115
  XNET troubleshooting 127
TSID code 9, 15
TSN 8

accessing support 15
available services 9
registering for services 9, 13
service charges 12
services 9
supported products 11

U
Unified IP client for Sun Ray, troubleshooting 152

V
Video conferencing parameters, configuring 198
Viewing, parameters on IP phones 193
Visual voice mail 145
VLAN ID, invalid 70
Voice mail 142
networked 149
ports show out of service 88, 89
resiliency 166
Voice networking, troubleshooting 155
Voice quality
monitoring and statistics 190
statistics 115
Volume setting on phone lost 55

W
Waiting for link 74
Web browser error, on Webset phones 61

X
XF86Config file 152
XNET troubleshooting 127
XRTC logs 17

Y
YA Phones, headset issues 60

GLOBAL HEADQUARTERS	U.S.	EMEA	CALA	ASIA PACIFIC
Tel: +1(613) 592-2122 Fax: +1(613) 592-4784	Tel: +1(480) 961-9000 Fax: +1(480) 961-1370	Tel: +44(0)1291-430000 Fax: +44(0)1291-430400	Tel: +1(613) 592-2122 Fax: +1(613) 592-7825	Tel: +61(0) 2 9023 9500 Fax: +61(0) 2 9023 9501

FOR MORE INFORMATION ON OUR WORLDWIDE OFFICE LOCATIONS, VISIT OUR WEBSITE AT **MITEL.COM/OFFICES**

mitel.com